Руководство по настройке коммутаторов
серия QSW-3750

Оглавление

1. НАЗНАЧЕНИЕ И АУДИТОРИЯ

В этом документе описывается интерфейс командной строки (CLI), используемый для настройки и мониторинга работы программного обеспечения коммутатора. Доступ к командной строке можно получить при помощи прямого подключения к последовательному порту коммутатора либо по Telnet или SSH через удаленное подключение.

Этот документ предназначен для системных администраторов, настраивающих и эксплуатирующих коммутаторы QTECH. Документ содержит описание конфигурации ПО коммутатора.

Предполагается, что читатель понимает базовые принципы работы программного обеспечения коммутатора и ознакомлен с техническими характеристиками соответствующего устройства. Также предполагается, что читатель обладает базовыми знаниями о технологии Ethernet и пониманием механизмов работы компьютерных сетей.

Пожалуйста, ознакомьтесь с техническим описанием коммутаторов. Техническое описание содержит информацию о характерных для конкретных коммутаторов функциях маршрутизации, коммутации, SNMP, настроек, управления и других функциях. Некоторые функции не поддерживаются в определенных моделях коммутаторов.

2. ОПИСАНИЕ ПО КОММУТАТОРА

Описание ПО коммутатора

Программное обеспечение коммутатора выполняет две функции:

- Обеспечивает различные возможности коммутации фреймов, основываясь на содержащейся в них информации 2,3 и 4 уровней OSI.
- Предоставляет сетевому администратору возможности для мониторинга и конфигурирования.

2.1. Описание продукта

Развитие сетевых технологий перевело коммутацию Fast Ethernet и Gigabit Ethernet из класса магистральных приложений уровня high-end в разряд недорогих потребительских решений. Стоимость решений продолжает снижаться, и в то же время повышается производительность и расширяется набор доступных функций. Устройства, способные осуществлять коммутацию уровней 2, 3 и 4 OSI, становятся все более востребованы. Программное обеспечение коммутатора обеспечивает гибкое решение для этих все возрастающих потребностей.

Точные функциональные возможности каждого сетевого устройства, на котором работает базовое ПО коммутатора, отличаются в зависимости от модели. В любом случае, ПО включает в себя набор функций для управления как самим коммутатором, так и сетью. Вы можете управлять ПО одним из следующих трех способов:

- Интерфейс командной строки (CLI)
- Simple Network Management Protocol (SNMP)
- Веб-интерфейс

Каждый из данных способов позволяет работать как локально, так и удалённо, используя механизмы управления по внутреннему или по вспомогательному каналу. Управление основывается на стандартах, с параметрами конфигурации и приватной MIB, обеспечивающими возможность управления функциями, не полностью описанными в публичных MIB.

3. РАБОТА С ИНТЕРФЕЙСОМ КОМАНДНОЙ СТРОКИ

Интерфейс командной строки (CLI) представляет собой стредство конфигурирования и мониторинга состояния системы, основанное на текстовых командах. Доступ к командной строке можно получить при помощи прямого подключения к последовательному (консольному) порту, либо при помощи удалённого логического соединения посредством Telnet или SSH.

Данный раздел описывает синтаксис командной строки, условные обозначения и командные режимы. Раздел содержит следующие секции:

- Синтаксис команд
- Условные обозначения команд
- Общие значения параметров
- Правила наименования unit/slot/port
- Использование «No»-формы команд
- Режимы командной строки
- Сокращенная форма и автозавершение команд
- Сообщения об ошибках CLI
- Комбинации клавиш для работы в командной строке
- Справка и поддержка в командной строке
- Получение доступа к CLI

3.1. Синтаксис команд

Команда – это одно или несколько слов, за которыми могут следовать один или несколько параметров. Параметры могут быть обязательными или необязательными.

Некоторые команды, например **show network** или **clear vlan**, не требуют указания параметров. С другими командами, такими как network parms, требуется указать обязательный параметр. Параметры следует указывать в строгом порядке. Сначала указываются обязательные параметры, затем – необязательные. Ниже приведен пример, иллюстрирующий синтаксис команды **network parms**:

network parms ipaddr netmask ***[gateway]***

- **network parms** – это имя команды.
- **ipaddr и netmask** – это параметры, вместо которых необходимо ввести нужные значения, после ввода ключевых слов команды.
- **[gateway]** – это необязательный параметр. Вы можете указать его значение, а можете не указывать.

Справочник команд содержит все команды, вместе с именем команды и кратким описанием её работы. Описание каждой команды содержит следующую информацию:

- **Формат** – показывает ключевые слова команды, а также необходимые и необязательные параметры.
- **Режим** – указывается режим CLI, необходимый для исполнения команды.
- **По умолчанию** – указываются значения по умолчанию, если таковые имеются, для данной команды.

Команды **show** содержат также описание информации, которую данная команда может вывести на экран.

3.2. Условные обозначения команд

Параметры команд могут включать в себя обязательные значения, необязательные значения либо одно из ключевых слов. Параметры указываются в строгом порядке. Таблица 1 описывает условные обозначения, принятые в данном документе для разграничения значений различных типов.

Таблица 1. Обозначение

Символ	Пример	Описание
[] квадратные скобки	[value]	Необязательный параметр.
Курсив	value или [value]	Значение переменной. Текст, выделенный курсивом, необходимо заменить на нужное значение, которое может представлять собой строку текста или число.
{} фигурные скобки	{choice1 | choice2}	Необходимо выбрать один из перечисленных параметров.
| вертикальная черта	choice1 | choice2	Разделяет взаимоисключающие варианты.
[{}] фигурные скобки внутри квадратных	[{choice1 | choice2}]	Выбор одного из необязательных параметров.

3.3. Общие значения параметров

Значения параметров могут представлять собой строку текста или число. Если в составе текстового значения параметра присутствует пробел - заключите значение в кавычки. Например, выражение **“System Name with Spaces”** заставляет систему принять значение с пробелами. Определяемые пользователем значения не могут представлять собой пустую строку (**""**). Таблица 2 описывает общие значения параметров и различные типы форматирования.

Таблица 2. Описание параметров

Параметры	Описание
ipaddr	Действительный IP-адрес. IP-адрес вводится в одном из следующих форматов: (32 бита) (8.24 бита) (8.8.16 бит) a.b.c.d (8.8.8.8) В дополнение к этим форматам, командная строка принимает десятичный, шестнадцатеричный и восьмеричный форматы, через следующие форматы ввода (где n - любое действительное шестнадцатеричное, восьмеричное или десятичное число): 0xn (командная строка принимает шестнадцатеричный формат). 0n (командная строка принимает восьмеричный формат с нулями). n (командная строка принимает десятичный формат).
Адрес IPv6	FE80:0000:0000:0000:020F:24FF:FEBF:DBCB, или FE80:0:0:0:20F:24FF:FEBF:DBCB, или FE80::20F24FF:FEBF:DBCB, или FE80:0:0:0:20F:24FF:128:141:49:32 Дополнительные сведения см. в RFC 3513.
Интерфейс или unit/slot/port	Номера слота и порта разделяются косой чертой. Например, 0/1 обозначает номер слота 0 и номер порта 1.
Логический интерфейс	Представляет собой логические номера слота и порта. Это применимо в случае агрегированных каналов (LAG). Вы можете использовать логический unit/slot/port для настройки агрегированного канала.
Строки символов	Используйте двойные кавычки для обозначения строки символов, например, "System name with Spases". Пустая строка ("") недопустима.

3.4. Правила наименования unit/slot/port

ПО коммутатора обращается к физическим объектам, таким как платы и порты, с использованием правила unit/slot/port. Данное правило применяется и для идентификации логических объектов, например, интерфейсов агрегированного канала.

Номер слота может означать одно из двух, в зависимости от случая применения. В случае с физическим портом он указывает на плату, содержащую данный порт. В случае с логическим портом и портом CPU он также идентифицирует тип интерфейса или порт.

Таблица 3. Типы слотов

Тип слота	Описание
Нумерация физических слотов	Нумерация физических слотов начинается с нуля и заканчивается номером последнего нумеруемого порта на устройстве.
Нумерация логических слотов	Логические слоты немедленно следуют за физическими слотами и идентифицируют агрегированные каналы (LAG) или интерфейсы маршрутизатора. Значение номера логического слота зависит от типа логического интерфейса и может отличаться от платформы к платформе.
Нумерация слотов CPU	Слоты CPU немедленно следуют за логическими слотами.

Порт идентифицирует конкретный физический порт или логический интерфейс, управление которыми осуществляется, на данном слоте.

Таблица 4. Типы портов

Тип порта	Описание
Физические порты	Физические порты для всех слотов нумеруются последовательно, начиная с единицы. Например, порт 1 в слоте 0 (внутренний порт) для отдельно стоящего (не состоящего в стеке) коммутатора) будет иметь номер 1/0/1, порт 2 – 1/0/2, порт 3 - 1/0/3, и так далее.
Логические интерфейсы	Интерфейсы агрегированного канала (или группы каналов) представляют собой логические интерфейсы, которые используются только для функции моста. VLAN-интерфейс используется только для функций маршрутизации. Loopback-интерфейсы являются логическими интерфейсами, потоянно находящиеся в рабочем состоянии. Туннельные интерфейсы – это логические линки точка-точка, пересылающие инкапсулированные пакеты.
Порты CPU	Порты CPU используются драйвером либо другим физическим объектом, расположенным на физических слотах.

ПРИМЕЧАНИЕ: В командной строке loopback-интерфейсы и туннельные интерфейсы не используют формат **unit/slot/port**. Для выделения loopback-интерфейса используете loopback ID. Для выделения туннельного интерфейса используйте tunnel ID.

3.5. Использование «No»-формы команд

Ключевое слово «no» позволяет использовать специальную форму существующей команды (и не является командой самостоятельно). Почти каждая команда конфигурации

имеет форму «no». В общем случае команда с ключевым словом «no» делает противоположное этой же команде без ключевого слова «no», либо возвращает значение по умолчанию. Например, команда **no shutdown** отменяет выключение интерфейса. Используйте команду без ключевого слова «no», чтобы повторно включить отключенный функционал или вклюючить функционал выключенный по умолчанию. «No»-форму имеют только конфигурационные команды.

3.6. Выполнение команд "show"

Все команды «**show**» можно вызвать в любом режиме (режиме Global Configuration, Interface Configuration, VLAN Configuration и т.п.). Команды «**show**» выводят информацию об определенном параметре системы, его состоянии, текущей конфигурации и статистике. Ранее команды «**show**» могли быть выполнены только в режимах User EXEC и Privileged EXEC.

3.7. Фильтрация вывода командной строки

Многие команды «**show**» выдают пользователю значительное количество информации. Это может показаться слишком запутанным и сложным для восприятия. Функция фильтрации выдачи позволяет пользователю указывать определенные аргументы, что помогает пользователю легче найти нужную информацию.

Главные фукнции фильтрации выдачи командной строки:

- Постраничная разбивка страниц
    - Поддерживается включение/отключение разбивки выдачи по страницам для всех команд «**show**». Если функция отключена, вывод отображается единым блоком. Если функция включена, вывод отображается страница за страницей таким образом, что информация не прокручивается на экране до тех пор, пока пользователь не нажмёт клавишу для продолжения. В конце каждой страницы отображается следующая подсказка: --More-- or (q)uit
    - Клавиши, используемые при включенной функции постраничной разбивки: Return (Enter) осуществляет отображение новой строки, q или Q отключают постраничную разбивку, любая другая клавиша переводит на следующую страницу. Переназначить функции на другие клавиши нельзя.

ПРИМЕЧАНИЕ: Хотя некоторые команды «**show**» сами по себе поддерживают постраничную разбивку, принцип разбивки может отличаться для различных команд этого типа.

- Фильтрация вывода
    - “**Grep**” – подобные команды, модифицирующие вывод таким образом, что пользователь видит лишь желаемый контент.
- Фильтрация, показывающая только те строки, которые содержат совпадения с заданным значением.
- Фильтрация, скрывающая из выдачи строки, которые содержат совпадения с заданным значением.
- Фильтрация, показывающая только те строки, которые содержат совпадения с заданным значением, и следующие за ними.
- Фильтрация, показывающая только указанные разделы содержимого (например, “**interface 0/1**”) с настраиваемым разделителем конца раздела.

- Фильтрация по текстовому значению не чувствительна к регистру.
- Разбивка на страницы (в случае, если она включена) также применяется к отфильтрованной выдаче.

Пример: В данном примере рассматривается использование ключевых слов, фильтрующих вывод командной строки, в применении к одной из команд «show».

```
(Routing) #show running-config ?
<cr>                    Press enter to execute the command.
|                       Output filter options.
<scriptname>            Script file name for writing active configuration.
all                     Show all the running configuration on the switch.
interface               Display the running configuration for specificed interface on the switch.

(Routing) #show running-config | ?
begin                   Begin with the line that matches
exclude                 Exclude lines that matches
include                 Include lines that matches
section                 Display portion of lines
```

Новые команды данной функции подробно рассмотрены в главе «Команды фильтрации вывода командной строки».

3.8. Режимы командной строки

В командной строке команды сгруппированы в различные режимы, в зависимости от выполняемых функций. Каждый режим поддерживает определенный компонент ПО. Команды определенного режима не доступны до тех пор, пока соответствующий режим не будет задействован (единственное отключение - команды режима User EXEC, которые могут выполняться и в режиме Privileged EXEC).

В каждом из режимов интерфейс выглядит несколько иначе, что позволяет мгновенно определить текущий режим. Таблица 5 содержит описания режимов и их визуальных различий.

ПРИМЕЧАНИЕ: Набор командных режимов, доступных на конкретном коммутаторе, может отличаться, в зависимости от версии установленного ПО.

Таблица 5. Режимы командной строки

Режим команд	Вид	Описание
User EXEC	Switch>	Содержит ограниченный набор команд для просмотра базовой системной информации.
Privileged EXEC	Switch#	Позволяет выполнение любой команды EXEC, войти в режимы VLAN Config и Global Config.

Режим команд	Вид	Описание
Global Config	Switch (Config)#	Содержит команды общей настройки и позволяет модифицировать уже работающую конфигурацию.
VLAN config	Switch (Vlan)#	Содержит команды конфигурации VLAN.
Interface Config	Switch (Interface *unit/slot/port*)# Switch (Interface Loopback *id*)# Switch (Interface Tunnel id)#	Управление работой интерфейса. Так же дает доступ к командам настройки виртуальных интерфейсов маршрутизации. Используйте данный режим, для настройки физического порта или заданного логического интерфейса.
Interface Config	Switch (Interface *unit/slot/port(star trange)-unit/slot/port(end range)#*	Так же в данном режиме вы можете настраивать диапазон интерфейсов. Например: Switch (Interface 1/0/1-1/0/4) #
	Switch (Interface lag *lag-intfnum*)#	Переход в режим конфигурации интерфейса LAG
	Switch (Interface vlan vlan-id)#	Переход в режим конфигурации VLAN для указанного VLAN ID
Line Console	Switch (config-line)#	Содержит команды для настройки консольного интерфейса, в том числе настройки аутентификации.
Line SSH	Switch (config-ssh)#	Содержит команды для настройки протокола SSH, в том числе настройки аутентификации.
Line Telnet	Switch (config-telnet)#	Содержит команды для настройки протокола Telnet, в том числе настройки аутентификации.
AAA IAS User config	Switch (Config-IAS-User)#	Позволяет настроить пользовательский пароль в базе IAS.
Mail Server Config	Switch (Mail-Server)#	Позволяет настроить сервер электронной почты.

Режим команд	Вид	Описание
Policy Map Config	Switch (Config-policy-map)#	Содержит команды настройки карты политик QoS.
Policy Class Config	Switch (Config-policy-class-map)#	Режим создания, удаления и настройки карты политик классов. Команды отбора по классам классов работают как с общими критериями, так и с критериями уровней 2 и 3.
Class Map Config	Switch (Config-class-map)#	Режим включает команды настройки карты классов QoS.
Radius Dynamic Authorization Config	(Config-radius-da)	Режим настройки динамической авторизации RADIUS.
MAC Access-list Config	Switch (Config-mac-access-list)#	Позволяет создать список досутпа с фильтрацией по MAC, а также войти в режим конфигурации, содержащий команды, относящиеся к спискам такого рода.
TACACS Config	Switch (Tacacs)#	Содержит команды для настройки сервера TACACS.
DHCP Pool Config	Switch (Config dhcp-pool)#	Содержит команды настройки пула IP-адресов DHCP.
Support Mode	Switch (Support)#	Обеспечивает доступ к командам поддержки (режим должен использоваться только специалистами службы технической поддержки производителя, так как неправильное использование может стать причиной некорректной работой системы и/или прекращения гарантийных обязательств).

Таблица 6 описывает процедуру входа в каждый режим и выхода из него.

Таблица 6. Режимы командной строки, вход и выход

Режим команд	Метод доступа	Выход или вход в предыдущий режим
User EXEC	Первый уровень доступа	Для выхода введите **logout**.

Режим команд	Метод доступа	Выход или вход в предыдущий режим
Privileged EXEC	В режиме User EXEC введите **enable**.	Для выхода в режим User EXEC введите **exit** или нажмите Ctrl-Z.
Global Config	В режиме Privileged EXEC введите **configure**.	Для выхода в режим Privileged EXEC введите **exit** или нажмите Ctrl-Z.
VLAN Config	В режиме Privileged EXEC введите **vlan database**.	Для выхода в режим Privileged EXEC введите **exit** , или нажмите Ctrl-Z
Interface Config	В режиме Global Config введите: **interface unit/slot/port либо interface loopback id либо interface tunnel id interface unit/slot/port(startrange) -unit/slot/ port(endrange)** **interface lag** *lag-intf-num* **interface vlan** *vlan-id*	Для выхода в режим Global Config введите **exit**. Для выхода в режим Privileged EXEC введите **exit** или нажмите Ctrl-Z.
Line Console	В режиме Global Config введите **line console**:	Для выхода в режим Global Config введите **exit**. Для выхода в режим Privileged EXEC нажмите Ctrl-Z.
Line SSH	В режиме Global Config введите **line ssh**:	Для выхода в режим Global Config введите **exit**. Для выхода в режим Privileged EXEC нажмите Ctrl-Z.
Line Telnet	В режиме Global Config введите **line telnet**:	Для выхода в режим глобальной конфигурации введите **exit**. Для выхода в режим Privileged EXEC нажмите Ctrl-Z.
AAA IAS User Config	В режиме Global Config введите **aaa ias-user username name.**	Для выхода в режим Global Config введите **exit**. Для выхода в режим Privileged EXEC нажмите Ctrl-Z.
Mail Server Config	В режиме Global Config введите **mail-server address.**	Для выхода в режим Global Config введите **exit**. Для выхода в режим Privileged EXEC нажмите Ctrl-Z.

Режим команд	Метод доступа	Выход или вход в предыдущий режим
Policy-Map Config	В режиме Global Config введите **policy-map**.	Для выхода в режим Global Config введите **exit**. Для выхода в режим Privileged EXEC нажмите Ctrl-Z.
Policy-Class-Map Config	В режиме Policy Map введите **class**.	Для выхода в режим Policy Map введите **exit**. Для выхода в режим Privileged EXEC нажмите Ctrl-Z.
Class-Map Config	В режиме Global Config введите **class-map**. См. “class-map ”.	Для выхода в режим Global Config введите **exit**. Для выхода в режим Privileged EXEC нажмите Ctrl-Z.
MAC Access-list Config	В режиме Global Config введите **mac access-list extended name**.	Для выхода в режим Global Config введите **exit**. Для выхода в режим Privileged EXEC нажмите Ctrl-Z.
TACACS Config	В режиме Global Config введите **tacacs-server host ip-addr**, где **ip-addr** – это IP-адрес TACACS-сервера вашей сети.	Для выхода в режим Global Config введите **exit**. Для выхода в режим Privileged EXEC нажмите Ctrl-Z.
DHCP Pool Config	В режиме Global Config введите **ip dhcp pool pool-name**.	Для выхода в режим Global Config введите **exit**. Для выхода в режим Privileged EXEC нажмите Ctrl-Z.

Режим команд	Метод доступа	Выход или вход в предыдущий режим
Support Mode	В режиме Privileged EXEC введите **support**. **ПРИМЕЧАНИЕ:** Команда support доступна только после предварительно выполеннной команды **techsupport enable**.	Для выхода в режим Privileged EXEC введите **exit** или нажмите Ctrl-Z.

3.9. Сокращенная форма и автозавершение команд

Автозавершение команд заканчивает написание команды при вводе достаточного количества символов, позволяющих однозначно идентифицировать ключевое слово. После того как вы ввели достаточно букв, нажмите клавишу пробел или TAB для завершения слова.

Сокращенная форма позволяет выполнить команду после ввода достаточного количества символов, позволяющих однозначно ее идентифицировать. Перед выполнением команды необходимо ввести все обязательные для нее ключевые слова и параметры.

3.10. Сообщения об ошибках CLI

Ввод команды, которую система не может выполнить, вызывает сообщение об ошибке. Таблица 7 описывает наиболее распространенные сообщения об ошибках интерфейса командной строки.

Таблица 7. Сообщения об ошибках CLI

Текст сообщения	Описание
% Invalid input detected at '^' marker.	Указывает на ввод неверной или недоступной команды. Символ карет (^) показывает, где именно обнаружен некорректный текст. Это же сообщение появляется, если какой-то из параметров или значений не распознаётся.
Command not found / Incomplete command. Use ? to list commands.	Указывает на отсутствие обязательных ключевых слов или значений.
Ambiguous command	Оповещает о том, что введенных символов недостаточно для однозначной идентификации команды.

3.11. Комбинации клавиш для работы в командной строке

В Таблица 8 приведены комбинации клавиш, которые можно использовать для редактирования команд или увеличения скорости ввода команд. Вы также можете получить доступ к этому списку из интерфейса командной строки, введя help в режимах User или Privileged EXEC.

Таблица 8. Клавиатурные сокращения командной строки

Сочетание клавиш	Описание
DEL или BACKSPACE	Удалить предыдущий символ.
Ctrl-A	Перейти к началу строки.
Ctrl-E	Перейти в конец строки.
Ctrl-F	Перейти на один символ вперед.
Ctrl-B	Перейти на один символ назад.
Ctrl-D	Удаление текущего символа.
Ctrl-U, X	Удалить начало строки.
Ctrl-K	Удалить конец строки.
Ctrl-W	Удалить предыдущее слово.
Ctrl-T	Поменять местами текущий и следующий символы.
Ctrl-P	Перейти к предыдущей строке в буфере истории.
Ctrl-R	Заменить или вставить строчку.
Ctrl-N	Перейти к следующей строке в буфере истории.
Ctrl-Y	Напечатать последний удаленный символ.
Ctrl-Q	Включить последовательный поток.
Ctrl-S	Отключить последовательный поток.
Ctrl-Z	Выйти в предшествующий режим командной строки.
Tab, пробел	Автозавершение команды.
Exit	Возвращение в предыдущий режим.
?	Список доступных команд, ключевых слов или параметров.

3.12. Справка и поддержка в командной строке

Введите вопросительный знак (?) в командной строке для отображения списка доступных команд в текущем режиме.

```
(switch) >?
enable          Enter into user privilege mode.
help            Display help for various special keys.
logout          Exit this session. Any unsaved changes are lost.
password        Change an existing user's password.
ping            Send ICMP echo packets to a specified IP address.
quit            Exit this session. Any unsaved changes are lost.
show            Display Switch Options and Settings.
telnet          Telnet to a remote host.
```

Введите вопросительный знак (?) после слова, чтобы увидеть доступные для него параметры или ключевые слова.

```
(switch) #network ?
ipv6            Configure IPv6 parameters for system network.
javamode        Enable/Disable.
mac-address     Configure MAC Address.
mac-type        Select the locally administered or burnedin MAC address.
mgmt_vlan       Configure the Management VLAN ID of the switch.
parms           Configure Network Parameters of the device.
protocol        Select DHCP, BootP, or None as the network config protocol.
```

Если справочная информация содержит параметр, заключенный в угловые скобки, необходимо заменить его на значение. (Routing) #network parms ?

```
<ipaddr>        Enter the IP Address.
none            Reset IP address and gateway on management interface
```

Если у команды нет дополнительных ключевых слов и параметров, либо если параметры не являются обязательными, вы увидите следующее сообщение:

```
<cr>            Press Enter to execute the command
```

Можно также ввести знак вопроса (?) после ввода одного или нескольких символов в слове, чтобы вывести список доступных команд или параметров, которые начинаются с введенной последовательности символов, как показано в следующем примере:

```
(switch) #show m?
mac             mac-addr-table          mac-address-table
mail-server     mbuf                    monitor
```

3.13. Получение доступа к CLI

Доступ к командной строке можно получить при помощи прямого подключения к консольному порту, либо при помощи удалённого соединения посредством протоколов Telnet или SSH.

Для первоначального подключения, вы должны использовать прямое подключение к консольному порту. Вы не можете получить доступ к удаленной системе, в системе не настроены IP-адрес, маска подсети и шлюз по умолчанию. Вы можете ввести эти настройки вручную, либо получить их с сервера BOOTP или DHCP в вашей сети. Для получения дополнительной информации см. раздел "Команды сетевых интерфейсов".

4. РАЗДЕЛ: КОМАНДЫ СТЕКИРОВАНИЯ

В этой главе описываются команды стекирования, доступные в CLI.

Раздел состоит из следующих глав:

- Стекирование выделенных портов
- Команды стекирования портов

ВНИМАНИЕ: В ДАННОМ РАЗДЕЛЕ КОМАНДЫ ДЕЛЯТСЯ НА ДВЕ ФУНКЦИОНАЛЬНЫЕ ГРУППЫ:

1. Команды информации отображают настройки коммутатора, статистику и прочую информацию.
2. Команды конфигурации вносят изменения в настройки коммутатора. Каждой команде конфигурации соответствует команда информации, показывающая текущие настройки.

ПРИМЕЧАНИЕ: Основной коммутатор управления – коммутатор, управляющий стеком.

4.1. Стекирование выделенных портов

В этом разделе описаны команды, который используется для настройки стекирования выделенного порта.

stack

Эта команда устанавливает режим Stack Global Config.

Формат stack

Режим Global Config

member

Команда конфигурации. **unit** – идентификатор коммутатора, который должен быть добавлен в стек или удалён из него. **switchindex** – индекс из базы данных поддерживаемых типов коммутаторов. Индекс представляет собой 32-битное целое число. Данная команда выполняется на основном коммутаторе управления.

Формат member unit switchindex

Режим Stack Global Config

ПРИМЕЧАНИЕ: Выяснить поддерживаемые индексы коммутатора можно выполением на нем команды «show supported switchtype» в режимах User EXEC или Privileged EXEC.

no member

Эта команда удаляет устройство из стека. **unit** - идентификатор коммутатора, который должен быть удалён из стека. Данная команда выполняется на основном коммутаторе управления.

Формат no member *unit*

Режим Stack Global Config

switch priority

Данная команда позволяет настроить параметр, согласно которому определенному устройству назначается роль главного коммутатора управления. **unit** - идентификатор коммутатора. **Value** - параметр, позволяющий указать приоритет, который назначит порядок, в котором коммутаторы будут становиться главными коммутаторами управления в случае недоступности существующего. Диапазон значений - от 1 до 15. Коммутатор с более высоким приоритетом будет выбран на роль основного коммутатора управления в том случае, если активный основной коммутатор управления выйдет из строя. По умолчанию коммутаторы имеют значение 1. Коммутаторы, не имеющие аппаратной возможности стать главным блоком управления, не могут назначаться на эту роль.

По умолчанию включен

Формат switch *unit* priority *value*

Режим Global Config

switch renumber

Эта команда позволяет изменить идентификатор коммутатора в стеке. **oldunit** - текущий идентификатор коммутатора, который планируется изменить. **newunit** - новое значение идентификатора. В результате выполнения команды, коммутатор будет настроен с конфигурационной информацией для нового коммутатора, если таковая имеется. Предыдущая конфигурация, однако, будет храниться до отключения коммутатора. Данная команда выполняется на основном коммутаторе управления.

ПРИМЕЧАНИЕ: Если изменени идентификатор коммутатора управления, текущая конфигурация перестаёт использоваться (то есть стек работает так, как будто конфигурация была очищена).

Формат switch *oldunit* renumber *newunit*

Режим Global Config

movemanagement

Эта команда перемещает роль главного коммутатора управления с одного коммутатора на другой. **fromunit** – идентификатор текущего коммутатора управления. **tounit** – идентификатор нового коммутатора управления. После исполнения, весь стек в целом (включая все интерфейсы в стеке) будет настроен с использованием конфигурации на новом главном коммутаторе управления. После перезагрузки все функции коммутатора управления будут выполняться на новом устройстве. Для сохранения текущей конфигурации стека, перед сменой блока управления выполните следующую команду (в режиме Privileged EXEC): «**running-config nvram:startup-config**». Изменение главного коммутатора управления влечет за собой потерю всех маршрутов и адресов 2 уровня. Данная команда выполняется на главном коммутаторе управления. Перед выполением команды система предложит вам подтвердить своё решение.

Формат movemanagement *fromunit tounit*

Режим Stack Global Config

standby

Эта команда используется для настройки устройства в качестве резервного коммутатора управления (STBY).

ПРИМЕЧАНИЕ: Текущий главный коммутатор управления не может быть назначен также и резервным. Коммутатор, назначаемый на роль резервного коммутатора управления, должен поддерживать соответствующий функционал.

Формат standby *unit number*

Режим Stack Global Config

Параметры	Описание
Standby Management Unit Number	Номер (идентификатор) устройства, который должен быть назначен на роль резервного управляющего коммутатора. Необходимо указать действительный номер существующего устройства.

no standby

«No»-форма данной команды запускает логику автоматического выбора коммутатора на роль резервного управляющего коммутатора.

Формат no standby

Режим Stack Global Config

slot

Данная команда позволяет сконфигурировать слот в системе. **unit/slot** - идентификатор слота. **Cardindex** - индекс из базы данных поддерживаемых типов плат, указывающий тип платы, настроенный на конкретном слоте. Индекс представляет собой 32-битное целое число. Если плата подключена в ненастроенный слот, текущая информация будет удалена и слот будет перенастроен согласно конфигурации по умолчанию для данной платы.

Формат slot unit/slot cardindex

Режим Global Config

ПРИМЕЧАНИЕ: Выяснить поддерживаемые индексы можно выполнением команды «show supported cardtype» в режимах User EXEC или Privileged EXEC.

no slot

Данная команда удаляет настройки из существующего слота в системе.

Формат no slot unit/slot cardindex

Режим Global Config

ПРИМЕЧАНИЕ: Выяснить поддерживаемые индексы можно выполнением команды «**show supported cardtype**» в режимах User EXEC или Privileged EXEC.

set slot disable

Данная команда позволяет настроить административный режим слота (одного или нескольких). Если указать [all], команда применяется для всех слотов, в противном случае команда применяется к слоту, определенному в *unit/slot*.

Если плата или другой модуль присутствуют в слоте, этот административный режим будет применен к ним. Если слот пуст, этот административный режим будет применяться к любому вставленному в слот модулю. Если плата отключена, все порты на устройстве оперативно отключаются и начинают отображаться на экране управления как неактивные («unplugged»).

Формат set slot disable [*unit/slot]* | all]

Режим Global Config

no set slot disable

Данная команда позволяет отменить конфигурацию административного режима слота (одного или нескольких). Если указанть all, команда применяется для всех слотов, в противном случае команда применяется к слоту, определенному в **unit/slot**.

Если плата или другой модуль присутствуют в слоте, этот административный режим удаляет конфигурацию из содерижимого слота. Если слот пуст, этот административный режим удаляет конфигурацию с любого вставленного в слот модуля. Если плата отключена, все порты на устройстве оперативно отключаются и начинают отображаться на экране управления как неактивные («unplugged»).

Формат no set slot disable [*unit/slot]* | all]

Режим Global Config

set slot power

Данная команда позволяет настроить режим питания слота(-ов) и позволяет устройству подавать питание на плату, находящуюся в слоте. Если указать **all**, команда применяется для всех слотов в противном случае команда применяется к слоту, определенному в unit/slot.

Используйте эту команду при установке или удалении платы. Если плата или другой модуль присутствуют в слоте, режим будет применен к ним. Если слот пуст, режим будет применяться к любому вставленному в слот модулю.

Формат set slot power [*unit/slot]* | all]

Режим Global Config

no set slot power

Данная команда удаляет настройку режима питания слота(-ов) и запрещает подачу питания на плату, находящуюся в слоте. Если указать **all**, команда применяется для всех слотов, в противном случае команда применяется к слоту, определенному в **unit/slot**.

Используйте эту команду при установке или удалении платы. Если плата или другой модуль присутствуют в слоте, команда будет применена к ним. Если слот пуст, питание не будет подаваться на любой вставленный в слот модуль.

Формат no set slot power [*unit/slot]* | all]

Режим Global Config

reload (Stack)

Данная команда перезагружает весь стек либо отдельный коммутатор. **unit** - идентификатор коммутатора. Система попросит вас подтвердить свои действия.

Формат reload *[unit]*

Режим Priviledged EXEC

stack-status sample-mode

Данная команда используется для настройки глобального статуса режима управления и, опционально, размер выборки. Параметры режима и размера выборки применяются глобально ко всем коммутаторам в стеке. Режим по выборки по умолчанию – кумулятивное суммирование.

ПРИМЕЧАНИЕ: Данная команда конфигурации, применяется как часть функционала обслуживания, и, следовательно, не сохраняется при перезагрузках. Эта команда не отображается в текущей конфигурации ни при каких условиях. Пользователь должен самостоятельно переключать режим выборки при необходимости. При вводе эта команда применяется ко всем членам стека. Данная команда не применяется на коммутаторах вошедших в стек, после ее ввода.

По умолчанию Cumulative Summing

Формат stack-status sample-mode {cumulative | history} [max-samples *100 - 500*]

Режим Stack Global Config Mode

Параметры	Описание
sample-mode	Режим выборки
cumulative	Отслеживание суммы полученных смещений временых меток.
history	Отслеживание истории полученных временных меток.
max-samples	Максимальный хранимый размер выборки

ПРИМЕР:

Следующие команды переключают режим выборки на кумулятивное суммирование.

```
(Routing) #configure
(Routing) (Config)#stack
(Routing) (Config-stack)# stack-status sample-mode cumulative
```

ПРИМЕР:

Следующе команды переключают режим выборки на режим истории, и сбрасывает максимальный размер выборки на значение по умолчанию (300).

```
(Routing) #configure
(Routing) (Config)#stack
(Routing) (Config-stack)#stack-status sample-mode history
```

ПРИМЕР:

Следующие команды переключают режим выборки на режим истории, и устанавливает максимальный размер выборки 100.

```
(Routing) #configure
```

(Routing) (Config)#stack

(Routing) (Config-stack)#stack-status sample-mode history max-samples 100

show slot

Эта команда отображает информацию либо обо всех слотах в системе, либо о конкретном слоте.

Формат show slot *[unit/slot]*

Режим User EXEC

Privileged EXEC

Термин	Значение
Slot	Идентификатор слота в формате **unit/slot**.
Slot Status	Состояние: слот может быть пустым (empty), занятым (full) или в состоянии ошибки (error).
Admin State	Административный режим слота может быть включен (enabled) или отключен (disabled).
Power State	Режим питания слота может быть включен (enabled) или отключен (disabled).
Configured Card Model Identifier	Идентификатор модели платы в соответствии с настройками слота. Идентификатор модели состоит из 32 символов и используется для индентификации платы.
Pluggable	Плата в слоте может быть съемная либо не съемная.
Power Down	Указывает, может ли слот быть отключенным или нет.

После ввода значения **unit/slot** появится следующая информация:

Термин	Значение
Inserted Card Model Identifier	Идентификатор модели платы, подключенной в слот. Идентификатор модели состоит из 32 символов. Это поле отображается только в том случае, слот занят подключенной платой.
Inserted Card Description	Описание подключенной платы. Это поле отображается только в том случае, слот занят подключенной платой.
Configured Card Description	Описание настроенной платы.

show stack-status

Данная команда показывает тайминги heartbeat-сообщений, полученных коммутатором в стеке, и статистику потерь/отброшенных сообщений.

Формат show stack stack-status [*1-n* | all] [clear]

Режим Privileged EXEC

Ключевое слово	Описание
Current	Текущее время приема heartbeat-сообщения
Average	Среднее время полученных heartbeat-сообщений
Min	Минимальное время полученных heartbeat-сообщений
Max	Максимальное время полученных heartbeat-сообщений
Dropped	Счётчик потерянных/отброшенных heartbeat-сообщений

ПРИМЕР:

Данный пример показывает статистику heartbeat-сообщений для определенного коммутатора в стеке.

```
(Routing) #show stack-status
Stack Unit 1 Status
Sampling Mode: Cumulative Summing
---------------------------------------
Unit Current Average Min  Max  Dropped
---------------------------------------
```

show supported cardtype

Данная команда показывает информацию обо всех типах плат, либо об определенных их типах поддерживаемых системой.

Формат show supported cardtype [cardindex]

Режим User EXEC

Privileged EXEC

Если не указать значения для cardindex, вы получите следующий вывод:

Термин	Значение
Card Index (CID)	Индекс в базе поддерживаемых типов плат. Этот индекс используется во время предварительной настройки слота.
Card Model Identifier	Идентификатор модели для поддерживаемого типа платы.

Если указать значения для **cardindex**, вы получите следующий вывод:

Термин	Значение
Card Type	Тип платы, представляющий собой 32-битное число.
Model Identifier	Идентификатор модели для поддерживаемого типа платы.
Card Description	Описание поддерживаемого типа платы

show switch

Эта команда отображает информацию обо всех устройствах в стеке, либо о конкретном коммутаторе, если указано соответствующее значение.

Формат show switch [*unit*]

Режим Privileged EXEC

Термин	Значение
Switch	Идентификатор, назначенный коммутатору.

Если не указать значения для **unit** , вы получите следующие выходные данные:

Термин	Значение
Management Status	Указывает на то, является ли коммутатор: главным коммутатором управления, членом стека, настроенным резервным коммутатором, рабочим резервным коммутатором, либо же его статус не назначен.
Preconfigured Model Identifier	Идентификатор модели коммутатора, предназначенный для включения в стек. Идентификатор модели представляет собой 32-символьное поле, назначенное производителем для идентификации устройства.
Plugged-In Model Identifier	Идентификатор модели платы, подключенной в слот. Идентификатор модели представляет собой 32-символьное поле, назначенное производителем для идентификации устройства.
Switch Status	Состояние коммутатора. Возможные состояния таковы: OK, Unsupported, Code Mismatch, Config Mismatch или Not Present. Mismatch указывает, что коммутатор в стеке работает с другой версией прошивки, шаблона SDM либо с другой конфигурацией, нежели главный коммутатор управления. При запущенной синхронизации прошивок в стеке показывается статус «Updating Code».

Термин	Значение
Code Version	Обнаруженная на коммутаторе версия прошивки.

ПРИМЕР: Вывод командной строки для данной команды.

```
(switch) #show switch

SW       Management Switch   Standby Status   Preconfig Model ID   Plugged-in Model ID   Switch Status   Code Version

---------------------------------------------------------------------------------------

1        Mgmt SW                              BCM-56224            BCM-56224             OK              M.3.22.1

1        Stack Mbr           Oper Stby        BCM-56224            BCM-56224             OK              M.3.22.1
```

Если указать значения для unit, вы получите следующие выходные данные.

Термин	Значение
Management Status	Указывает на то, является ли коммутатор: главным коммутатором управления или членом стека, либо же его статус не назначен.
Hardware Management Preference	Аппаратное значение, согласно которому коммутатор получает управляющую роль. Может быть отключенным или не назначенным.
Admin Management Preference	Административное значение, согласно которому коммутатор получает управляющую роль. Указывает на вероятность выбора этого коммутатора на роль главного управляющего коммутатора.
Switch Type	Тип коммутатора (32-битное число)
Model Identifier	Идентификатор модели коммутатора. Идентификатор модели представляет собой 32-символьное поле, назначенное производителем для идентификации устройства.
Switch Status	Состояние коммутатора. Возможные значения: OK, Unsupported, Code Mismatch, Config Mismatch или Not Present.
Switch Description	Описание коммутатора.
Expected Code Type	Ожидаемый тип прошивки.

Термин	Значение
Expected Code Version	Ожидаемая версия прошивки.
Detected Code Version	Версия прошивки, работающая на коммутаторе. Если коммутатор отсутствует и данные получены от предварительной настройки, версией прошивки считается значение “None”.
Detected Code in Flash	Версия прошивки, в настоящий момент хранимая на FLASH-памяти коммутатора. Данная прошивка загружается после перезагрузки коммутатора. Если коммутатор отсутствует и данные получены от предварительной настройки, версией кода считается значение “None”.
SFS Last Attempt Status	Результат последней попытки синхронизации прошивок внутри стека, для конкретного устройства.
Serial Number	Серийный номер для указанного устройства.
Up Time	Время непрерывной работы системы.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Switching) #show switch 1
Switch ..... 1
Management Status..... Management Switch
Hardware Management Preference ..... Unassigned
Admin Management Preference..... Unassigned
Switch Type..... 0xb6240001
Preconfigured Model Identifier ..... Platform v1
Plugged-in Model Identifier..... Platform v1
Switch Status ..... STM Mismatch
Switch Description..... 56624 Development System  48 GE, 4 TENGIG
Expected Code Type ..... 0x100b000
Detected Code Version..... 10.17.15.8
Detected Code in Flash ..... 10.17.15.8
SFS Last Attempt Status ..... None
Up Time..... 0 days 3 hrs 15 mins 50 secs
```

show supported switchtype

Эта команда отображает информацию обо всех поддерживаемых типах коммутаторов (либо об определенном типе коммутаторов).

Формат show supported switchtype [switchindex]

Режим User EXEC

Privileged EXEC

Если не указать значения для **switchindex**, вы получите следующие данные:

Термин	Значение
Switch Index (SID)	Индекс в базе данных поддерживаемых коммутаторов. Данный индекс используется при добавлении преднастроенного коммутатора в стек.
Model Identifier	Идентификатор модели для поддерживаемого типа коммутатора.
Management Preference	Метрика приоритета управления для этого типа коммутаторов.
Code Version	Версия прошивки, ожидаемая для этого типа коммутаторов.

Если указать значения для **switchindex**, вы получите следующие данные:

Термин	Значение
Switch Type	Тип коммутатора, представляющий собой 32-битное число.
Model Identifier	Идентификатор модели для поддерживаемого типа коммутатора.
Switch Description	Описание поддерживаемого типа коммутатора.

4.2. Команды стекирования портов

В этом разделе описаны команды, которые используются для настройки стекирования портов и получения информации об этих портах.

stack-port

Данная команда настраивает режим стекирования для порта или диапазона портов. Доступные режимы **stack** или **ethernet**.

По умолчанию stack

Формат stack-port *unit/slot/port* [{ethernet | stack}]

Режим Stack Global Config

show stack-port

Данная команда отображает сводную информацию о стекируемых портах для всех интерфейсов.

Формат show stack-port

Режим Privileged EXEC

Для каждого интерфейса:

Термин	Значение
Unit	Номер устройства.
Interface	Номера слота и порта.
Configured Stack Mode	Stack или Ethernet.
Running Stack Mode	Stack или Ethernet.
Link Status	Состояние линка.
Link Speed	Скорость линка стекированных портов, в Гбит/с.

show stack-port counters

Данная команда отображает сводную информацию о счетчиках данных для всех интерфейсов.

Формат show stack-port counters [*1-n* | all]

Режим Privileged EXEC

Термин	Значение
Unit	Номер устройства.
Interface	Номера слота и порта.
Tx Data Rate	Скорость передачи данных на стекированном порте, в Мбит/с.
Tx Error Rate	Зависимое от платформы количество ошибок при передаче, в секунду.
Tx Total Errors	Зависимое от платформы количество ошибок при передаче, с момента включения.
Rx Data Rate	Скорость приема данных на стекированном порте, в Мбит/с.
Rx Error Rate	Зависимое от платформы количество ошибок при приеме, в секунду.

Термин	Значение
Rx Total Errors	Зависимое от платформы количество ошибок при приеме, с момента включения.
Link Flaps	Количество изменений состояния линка (рабочее/нерабочее), с момента загрузки системы.

ПРИМЕР: В этом примере показаны стекируемые порты и связанная с ними статистика устройства с номером 2.

```
(Routing) #show stack-port counters 2

TX                                                    RX
Data                        Error                     Data                        Error

Unit  Interface  Rate (Mb/s)  Rate (Errors/s)  Total Errors  Rate (Mb/s)  Rate (Errors/s)  Total Errors  Link Flaps
-------------------------------------------------------------------------------------------------------------
2     0/53       0            0                0             0            0                0             0
2     0/54       0            0                0             0            0                0             0
2     0/55       0            0                0             0            0                0             0
2     0/56       0            0                0             0            0                0             0

(Routing) #
```

show stack-port diag

Данная команда показывает диагностическую информацию о каждом порте и предназначена для инженеров технической поддержки. Она выполняется по указанию специалиста ТП и содержит счётчики для RPC, транспорта, CPU, модулей RX и TX.

Формат show stack-port diag [*1-n* | all] [verbose]

Режим Privileged EXEC

Термин	Значение
Unit	Номер устройства.
Interface	Номера слота и порта.
Diagnostic Entry1	Строка из 80 символов, используемая для диагностики.
Diagnostic Entry2	Строка из 80 символов, используемая для диагностики.

Термин	Значение
Diagnostic Entry3	Строка из 80 символов, используемая для диагностики.
TBYT	Количество переданных байт
TPKT	Количество переданных пакетов
TFCS	Счетчик ошибок контрольной суммы переданных фреймов
TERR	Счетчик ошибок при передаче (устанавливается системой)
RBYT	Количество полученных байт
RPKT	Количество полученных пакетов
RFCS	Счетчик ошибок контрольной суммы полученных фреймов
RFRG	Счетчик полученных фрагментов
RJBR	Счетчик полученных Jabber-фреймов
RUND	Счетчик полученных фреймов неполного размера
ROVR	Счетчик полученных фреймов избыточного размера
RUNT	Счетчик полученных карликовых фреймов

ПРИМЕР: В этом примере показаны стекируемые порты и связанная с ними статистика.

```
(Routing) #show stack-port diag 1
1 - 0/53:
RBYT:27ed9a7b RPKT:bca1b TBYT:28a0739e TPKT:c93ee
RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0
TFCS:0 TERR:0

1 - 0/54:
RBYT:8072ed RPKT:19a66 TBYT:aecfb80 TPKT:66e4d
RFCS:6e RFRG:4414 RJBR:0 RUND:c19 RUNT:af029b1
TFCS:0 TERR:0

1 - 0/55:
RBYT:0 RPKT:0 TBYT:ae8 TPKT:23
RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0
TFCS:0 TERR:0
```

1 - 0/56:

RBYT:0 RPKT:0 TBYT:ae8 TPKT:23

RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0

TFCS:0 TERR:0

Пример 2: 'show stack-port diag [<1-n> | all] [verbose]' статистика transport и т.д. модулей указанного устройства или всех устройств.

В этом примере показана статистика RPC, Transport (ATP, Next Hop, и RLink), CPU Transport и Rx/Tx модулей устройства с номером 2.

(Routing) #show stack-port diag 2 verbose –

----------HPC

RPC statistics/counters from unit..2

Registered Functions..... 58

Client Requests 0

Server Requests 0

Server Duplicate Requests..... 0

Server Replies..... 0

Client Remote Tx..... 0

Client Remote Retransmit Count 0

Tx without Errors..... 0

Tx with Errors 0

Rx Timeouts 0

Rx Early Exits..... 0

Rx Out of Sync 0

No Buffer..... 0

Collect Sem Wait Count 0

Collect Sem Dispatch Count 0

RPC statistics/counters from unit..2

Client RPC Requests Count..... 3

Client RPC Reply Count..... 0

Client RPC Fail to xmit Count 0

Client RPC Response Timedout Count..... 3

Client RPC Missing Requests 0

Client RPC Detach/Remove Count..... 0

Client RPC Current Sequence Number 3

Server RPC Request Count 0

Server RPC Reply Count..... 0
Server RPC Processed Transactions..... 0
Server RPC Received Wrong Version Req..... 0
Server RPC No Handlers..... 0
Server RPC Retry Transmit Count..... 0
Server RPC Repetitive Tx Errors 0

ATP statistics/counters from unit..2

Transmit Pending Count 2
Current number of TX waits..... 2
Rx transactions created 145
Rx transactions freed 145
Rx transactions freed(raw) 0
--More-- or (q)uitATP: TX timeout, seq 74. f:cc cli 778. to 1 tx cnt 21.
Tx transactions created 290
BET Rx Dropped Pkts Count..... 0
ATP Rx Dropped Pkts Count..... 0
Failed to Add Key Pkt Count..... 0
Source Lookup Failure Count..... 0
Old Rx transactions Pkts drop Count..... 0
Nr of CPUs found in ATP communication 2
----------CPU
Transport statistics/counters from unit..2

State Initialization ..... Done
Rx Setup..... Done
Tx Setup..... Done
Tx CoS[0] Reserve..... 100
Tx CoS[1] Reserve..... 100
Tx CoS[2] Reserve 100
Tx CoS[3] Reserve 100
Tx CoS[4] Reserve..... 60
Tx CoS[5] Reserve..... 40
Tx CoS[6] Reserve 20
Tx CoS[7] Reserve 0
Tx Pkt Pool Size 200

Tx Available Pkt Pool Size 198
Tx failed/error Coun 0
Rx Pkt Pool Size..... 8

Next Hop statistics/counters from unit..2

State Initialization ..... Done
Component Setup..... Done
Thread Priority..... 100
Rx Priority 105
Local CPU Key 00:24:81:d0:0f:c7
MTU Size..... 2048
Vlan Id 4094
CoS Id 7
Internal Priority for pkt transmission..... 7
Rx Pkt Queue Size..... 256
Tx Pkt Queue Size..... 64
Rx Pkt Dropped Count 0
Tx Failed Pkt Count..... 0

RLink statistics/counters from unit..2

State Initialization ..... Done
L2 Notify In Pkts..... 0
L2 Notify In Pkts discarded 0
L2 Notify Out Pkts 0
L2 Notify Out Pkts discarded 0
Linkscan In Pkts..... 0
Linkscan In Pkts discarded 0
Linkscan Out Pkts 0
Linkscan Out Pkts discarded 0
Auth/Unauth In Callbacks 0
Auth/Unauth In Callbacks discarded..... 0
Auth/Unauth Out Callbacks 0
Auth/Unauth Out Callbacks discarded..... 0
RX Tunnelling In Pkts..... 0
RX Tunnelling In Pkts discarded..... 0

```
RX Tunnelling Out Pkts..... 0
RX Tunnelling Out Pkts discarded ..... 0
OAM Events In..... 0
OAM Events In discarded ..... 0
OAM Events Out ..... 0
OAM Events Out discarded ..... 0
BFD Events In..... 0
BFD Events In discarded ..... 0
BFD Events Out ..... 0
BFD Events Out discarded ..... 0
Fabric Events In ..... 0
Fabric Events In discarded..... 0
Fabric Events Out..... 0
Fabric Events Out discarded..... 0
Scan Add Requests In..... 0
Scan Del Requests In..... 0
Scan Notify(Run Handlers) Out..... 0
Scan Notify(Traverse Processing)..... 0
(Routing) #
```

show stack-port stack-path

Данная команда отображает маршрут, который потребуется пакетам, чтобы достичь адреса назначения.

Формат show stack-port stack-path {*1-8* | *all*}

Режим Privileged EXEC

4.3. Команды синхронизации прошивок внутри стека

Синхронизация внутри стека (SFS) позволяет автоматически поддерживать одну и ту же версию прошивки для всех устройств в стеке. Если устройство включается к стек и его версия прошивки отличается от версии, работающей на управляющем устройстве, SFS установит на него нужную версию прошивки. При этом, система не будет пытаться использовать последнюю версию прошивки из тех, что встречаются на устройствах внутри стека.

boot auto-copy-sw

Используйте эту команду для включения функции синхронизации прошивок внутри стека.

По умолчанию Disabled (Отключено)

Формат boot auto-copy-sw

Режим Privileged EXEC

no boot auto-copy-sw

Используйте эту команду для отлючения функции синхронизации прошивок внутри стека.

Формат no boot auto-copy-sw

Режим Privileged EXEC

boot auto-copy-sw trap

Используйте эту команду для включения отправления SNMP-trap, относящихся к функции SFS.

По умолчанию Enabled

Формат boot auto-copy-sw trap

Режим Privileged EXEC

no boot auto-copy-sw trap

Используйте эту команду для отключения отправления SNMP-trap, относящихся к функции SFS.

Формат no boot auto-copy-sw trap

Режим Privileged EXEC

boot auto-copy-sw allow-downgrade

Используйте эту команду для того, чтобы управляющее устройство стека понижало версию прошивок, если их версия более новая, чем на управляющем устройстве.

По умолчанию Enabled

Формат boot auto-copy-sw allow-downgrade

Режим Privileged EXEC

no boot auto-copy-sw allow-downgrade

Используйте эту команду, чтобы запретить управляющему устройству стека понижать версию прошивки.

Формат no boot auto-copy-sw allow-downgrade

Режим Privileged EXEC

show auto-copy-sw

Данная команда отображает текущее состояние и настройки функции синхронизации прошивок внутри стека.

Формат show auto-copy-sw

Режим Privileged EXEC

Термин	Значение
Synchronization	Показывает, включена ли функция SFS.

Термин	Значение
SNMP Trap Status	Показывает, будет ли стек отправлять SNMP-trap.
Allow Downgrade	Показывает, разрешено ли управляющему устройству понижать версию прошивок устройств в стеке.

5. РАЗДЕЛ: КОМАНДЫ УПРАВЛЕНИЯ

В этой главе описываются управляющие команды, доступные в SMB CLI.

Раздел состоит из следующих глав:

ВНИМАНИЕ: В ДАННОМ РАЗДЕЛЕ КОМАНДЫ ДЕЛЯТСЯ НА ТРИ ФУНКЦИОНАЛЬНЫЕ ГРУППЫ:

1. Команды Show отображают настройки коммутатора, статистику и прочую информацию.
2. Команды конфигурации вносят изменения в настройки коммутатора. Каждой команде конфигурации соответствует команда информации (show), показывающая текущие настройки.
3. Команды Clear сбрасывают определенные настройки на заводские значения.

5.1. Команды сетевых интерфейсов

В этом разделе описываются команды, которые используются для настройки логического интерфейса для доступа к управлению. Для настройки управления VLAN см. раздел "Команды VLAN".

enable (Privileged EXEC access)

Данная команда предоставляет доступ в режим Privileged EXEC. В режиме Privileged EXEC вы можете конфигурировать сетевые интерфейсы.

Формат enable

Режим User EXEC

do (Privileged EXEC commands)

Данная команда выполняет команды режима Privileged EXEC из любого другого режима.

Формат do Priv Exec Mode Command

Режим Global Config

Interface Config

VLAN Config

Routing Config

ПРИМЕР: Ниже приведен пример команды «do», которая выполняет команду **script list** режима Privileged EXEC в режиме Global Config.

```
(Routing) #configure
(Routing)(config)#do script list
Configuration Script Name        Size(Bytes)
--------------------------------------------------
backup-config                    2105
running-config                   4483
startup-config                   4453
configuration script(s) found.
2041 Kbytes free. Routing(config)#
```

network parms

Эта команда устанавливает IP-адрес, маску подсети и шлюз. IP-адрес и шлюз должен быть в той же подсети. Параметр none устанавливает IP-адрес и маску подсети на заводские значения по умолчанию.

Формат network parms {*ipaddr netmask* [*gateway*]| none}

Режим Privileged EXEC

network protocol

Данная команда позволяет выбрать один из протоколов конфигурации сети. Измененные настройки вступают в силу немедленно. **bootp** - коммутатор начинает периодически отправлять запрос на BootP-сервер, до тех пор, пока не будет получен ответ. **dhcp** - коммутатор начинает периодически отправлять запрос на DHCP-сервер, до тех пор, пока не будет получен ответ. **none** - настройка параметров сети производится вручную.

По умолчанию none

Формат network protocol {none | bootp | dhcp}

Режим Privileged EXEC

network protocol dhcp

Эта команда включает DHCPv4-клиент на сетевом порте. **client-id** - необязательный параметр, заставляющий DHCP-клиент отправлять сообщения с идентификатором клиента.

По умолчанию none

Формат network protocol dhcp [client-id]

Режим Global Config

Форма **no** командой **network protocol dhcp client-id** не поддерживается. Для того, чтобы отменить опцию **clientid**, просто выполните команду **network protocol dhcp** (без опции **client-id**). Команда **network protocol none** отключает на интерфейсе как опцию **client-id**, так и сам DHCP-клиент.

ПРИМЕР: Ниже приведен пример команды.

(Routing) # network protocol dhcp client-id

network mac-address

Эта команда устанавливает локально администрируемый MAC-адрес. Применяются следующие правила:

- Бит 6 байта 0 (так называемый бит U/L) указывает на то, является ли адрес администрируемым универсально (b'0') или же администрируемым локально (b'1').
- Бит 7 байта 0 (так называемый бит I/G) указывает на то, является ли адрес индивидуальным (b'0') или групповым (b'1').
- Второй символ из 12 должен быть одним из следующих: 2, 6, A, E.

Локально администрируемый MAC-адрес должен иметь включенный бит 6 (b'1') и выключенный бит 7 (b'0').

Формат network mac-address *macaddr*

Режим Privileged EXEC

network mac-type

Эта команда определяет, будет коммутатор использовать заводской или же локально администрируемый MAC-адрес.

По умолчанию burnedin

Формат network mac-type {local | burnedin}

Режим Privileged EXEC

no network mac-type

Эта команда возвращает значение MAC-адреса на заводское.

Формат no network mac-type

Режим Privileged EXEC

network javamode

Эта команда указывает, должен ли коммутатор разрешить доступ к Java-апплету в Web-интерфейсе. Включенная опция позволяет видеть Java-апплет в Веб-интерфейсе. Отключенная опция, соответственно, не позволяет.

По умолчанию включен

Формат network javamode

Режим Privileged EXEC

no network javamode

Эта команда запрещает доступ к Java-апплету в Web-интерфейсе. Пользователь не видит апплет, если доступ отключен.

Формат no network javamode

Режим Privileged EXEC

show network

Эта команда отображает параметры конфигурации, связанные с сетевым интерфейсом коммутатора. Сетевой интерфейс - это логический интерфейс, используемый для внутриполосного подключения коммутатора через любой из портов на передней панели. Параметры конфигурации, связанные с сетевым интерфейсом коммутатора, не влияют на конфигурацию тех портов на передней панели, с помощью которых происходит коммутация и маршрутизация трафика. Сетевой интерфейс всегда считается запущенным, независимо от состояния принадлежащих к нему портов; поэтому команда **show network** всегда будет показывать **Interface Status** как Up.

Формат show network

Режимы Privileged EXEC

User EXEC

Термин	Значение
Interface Status	Состояние сетевого интерфейса; всегда считается "up".
IP Address	IP-адрес интерфейса. Значение по умолчанию - 0.0.0.0.
Subnet Mask	Маска подсети интерфейса. Значение по умолчанию - 0.0.0.0.
Default Gateway	Шлюз по умолчанию. Значение по умолчанию - 0.0.0.0.
IPv6 Administrative Mode	Может быть включенным или отключенным.
IPv6 Address/Length	Адрес IPv6 и длина.
IPv6 Default Router	Адрес маршрутизатора IPv6 по умолчанию.
Burned In MAC Address	Заводской MAC-адрес, используемый для внутриполосного соединения.

Термин	Значение
Locally Administered MAC Address	В случае необходимости, для внутриполосного соединения можно назначить локально администрируемый MAC-адрес. Для этого необходимо, чтобы опция «MAC Address Type» имела настройку «Locally Administered». Введите адрес, 12 шестнадцатеричных цифр (6 байт) с двоеточием после каждого байта. Бит 1 байта 0 необходимо установить на 1, бит 0 – на 0, таким образом, байт 0 должен иметь следующую маску: 'xxxx xx10'. MAC-адрес, используемый таком мосту, должен быть уникальным. Числовое значение MAC-адреса рекомендуется устанавливать меньше, чем значение MAC-адресов каждого порта, принадлежащего мосту. Однако, единственным обязательным требованием является уникальность адреса. При объединении с dot1dStpPriority, формируется уникальный Идентификатор Моста, который используется в Spanning Tree Protocol.
MAC Address Type	MAC-адрес, который будет использоваться для внутриполосного подключения. Возможные варианты: заводской или локально администрируемый адрес. По умолчанию выбран заводской адрес.
Configured IPv4 Protocol	Сетевой протокол IPv4. Возможные варианты: bootp | dhcp | none.
Configured IPv6 Protocol	Сетевой протокол IPv6. Возможные варианты: dhcp | none.
DHCPv6 Client DUID	Уникальный идентификатор клиента DHCPv6. Эта строка отображается только в том случае, если в настройках протокола IPv6 выбрано DHCP.
IPv6 Autoconfig Mode	Автоконфигурация IPv6 Stateless адреса - включена или отключена.
DHCP Client Identifier	Идентификатор клиента отображается только в том случае, если протокол DHCP включен с опцией client-id на сетевом порте. См. "network protocol dhcp ".

ПРИМЕР: пример вывода CLI отображающий настройки сетевого порта.

```
(admin) #show network
Interface Status..... Up
IP Address..... 10.250.3.1
Subnet Mask..... 255.255.255.0
Default Gateway..... 10.250.3.3
```

IPv6 Administrative Mode ..... Enabled
IPv6 Prefix is fe80::210:18ff:fe82:64c/64
IPv6 Prefix is 2003::1/128
IPv6 Default Router is..... fe80::204:76ff:fe73:423a
Burned In MAC Address 00:10:18:82:06:4C
Locally Administered MAC address..... 00:00:00:00:00:00
MAC Address Type..... Burned In
Configured IPv4 Protocol..... None
Configured IPv6 Protocol ..... DHCP
DHCPv6 Client DUID 00:03:00:06:00:10:18:82:06:4C
IPv6 Autoconfig Mode ..... Disabled
Management VLAN ID..... 1
DHCP Client Identifier..... 0fastpath-0010.1882.160B-vl1

5.2. Команды доступа консольного порта

В этом разделе описаны команды, используемые для настройки консольного порта. Вы можете использовать консольный кабель для подключения непосредственно к консольному порту коммутатора.

configure

Данная команда предоставляет доступ в режим Global Config. Из режима Global Config можно настроить самые разные параметры системы, в том числе учетные записи пользователей. Из этого режима возможно войти в другие, например, в режим Line Config.

Формат configure

Режим Privileged EXEC

line

Данная команда дает доступ к режиму Line Console, позволяющему настроить различные параметры Telnet и консольного порта, а также для настройки авторизации в консоли.

Формат line {console | telnet | ssh}

Режим lobal Config

Термин	Значение
console	Консольный терминал.
telnet	Виртуальный терминал для удаленного консольного доступа (Telnet).
ssh	Виртуальный терминал для защищённого удаленного консольного доступа (SSH).

ПРИМЕР: Ниже приведен пример команды.

```
(Routing)(config)#line telnet
(Routing)(config-telnet)#
```

serial baudrate

Эта команда задаёт скорость обмена данными интерфейса консольного порта. Поддерживаемые значения: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

По умолчанию 9600

Формат serial baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}

Режим line Config

no serial baudrate

Эта команда устанавливает скорость обмена данными интерфейса консольного порта по умолчанию.

Формат no serial baudrate

Режим Line Config

serial timeout

Эта команда указывает максимальное время соединения (в минутах) при отсутствии активности в консоли. Значение 0 означает, что консоль может быть подключена на неопределенный срок. Диапазон времени от 0 до 160.

По умолчанию 5

Формат serial timeout *0-160*

Режим Line Config

no serial timeout

Эта команда устанавливает максимальное время соединения (в минутах) при отсутствии активности в консоли.

Формат no serial timeout

Режим line Config

show serial

Эта команда отображает параметры подключения через последовательный порт.

Формат show serial

Режимы Privileged EXEC

User EXEC

Термин	Значение
Serial Port Login Timeout (minutes)	Время (в минутах) отсутствия активности, после которой коммутатор разрывает соединение. При значении 0 коммутатор не будет разрывать консольное соединение из-за отсутствия активности.
Baud Rate (bps)	Скорость по умолчанию (в бодах), с которой последовательный порт будет пытаться осуществить подключение.
Character Size (bits)	Количество битов на символ. Символ всегда состоит из 8 битов.
Flow Control	Включена или же отключена опция Hardware Flow-Control. Функция Hardware Flow-Control всегда отключена.
Stop Bits	Количество Stop-битов на символ. Количество Stop-битов всегда равно 1.
Parity	Метод проверки чётности, применяемый последовательным портом. Значение всегда None.

5.3. Команды Telnet

В этом разделе описаны команды, используемые для просмотра и изменения конфигурации Telnet. Telnet используется для дистанционного управления устройством.

ip telnet server enable

Данная команда используется для запуска Telnet-соединения и для включения режима Telnet Server Admin. Команда открывает порт, слушающий Telnet.

По умолчанию включен

Формат ip telnet server enable

Режим Global Config

no ip telnet server enable

Данная команда используется для отключения Telnet-соединения и режима Telnet Server Admin. Эта команда закрывает слушающий Telnet порт и разрывает все сесии Telnet.

Формат no ip telnet server enable

Режим Global Config

transport input telnet

Эта команда регулирует новые сеансы Telnet. Если эта функция включена, новые сеансы Telnet могут быть установлены до тех пор, пока не исчерпается лимит доступных сессий.

Установленная сессия считается активной до тех пор пока не закончится сеанс (в том числе из-за ошибок сети).

ПРИМЕЧАНИЕ: Если отключен режим Telnet Server Admin Mode, сеансы Telnet не могут быть установлены. Для включения этого режима воспользуйтесь командой **ip telnet server enable**.

По умолчанию включен

Формат transport input telnet

Режим Line Config

no transport input telnet

Используйте эту команду, чтобы запретить новые сеансы Telnet.

Формат no transport input telnet

Режим line Config

telnetcon maxsessions

Эта команда указывает максимальное количество сессий Telnet, которые могут быть установлены одновременно. Значение 0 указывает, что Telnet-соединение не может быть установлено. Диапазон: 0 – 5.

По умолчанию 5

Формат telnetcon maxsessions *0-5*

Режим Global Config

no telnetcon maxsessions

Эта команда сбрасывает максимальное количество одновременных сессий Telnet на заводские значения.

Формат no telnetcon maxsessions

Режим Global Config

telnetcon timeout

Эта команда устанавливает таймаут Telnet-сессии, в минутах. Сессия остаётся активной до тех пор, пока время неактивности не достигнет указанного значения. Таймаут указывается десятичным числом в диапазоне 1 – 160.

ПРИМЕЧАНИЕ: При изменении значения оно применяется немедленно ко всем активным и неактивным сессиям. Сессии, текущее время ожидания которых превышает новое значение таймаута, будут прекращены автоматически.

По умолчанию 5

Формат telnetcon timeout *1-160*

Режим Global Config

no telnetcon timeout

Эта команда сбрасывает значение таймаута Telnet-сессии на заводские установки.

ПРИМЕЧАНИЕ: Изменение времени сессии вступит в силу только для новых соединений. Каждая нажатая клавиша заново начинает отсчёт таймаута.

Формат no telnetcon timeout

Режим Global Config

show telnetcon

Эта команда отображает текущие входящие соединения Telnet. Другими словами, отображаться будут только те Telnet-соединения, которые были инициированы с удалённых устройств.

Формат show telnetcon

Режимы Privileged EXEC

User EXEC

Термин	Значение
Remote Connection Login Timeout (minutes)	Указывает на количество минут в режиме ожидания, после которых соединение будет разорвано. Может быть указано как число от 1 до 160. Значение по умолчанию - 5.
Maximum Number of Remote Connection Sessions	Это значение указывает на разрешенное количество одновременных подключений. Значение по умолчанию - 5.
Allow New Telnet Sessions	Новые сеансы Telnet не разрешается, если в этом поле задано значение «no». Значение по умолчанию - «yes».

5.4. Команды Secure Shell

В этом разделе описаны команды, который используется для настройки доступа к коммутатору через SSH. Используйте SSH для защищённого доступа к коммутатору с удаленного устройства.

ПРИМЕЧАНИЕ: Система разрешает до 5 сеансов SSH.

ip ssh

Используйте эту команду для включения доступа к системе по SSH. Данная команда - краткая версия команды ip ssh server enable.

По умолчанию disabled

Формат ip ssh

Режим Global Config

ip ssh protocol

Эта команда используется для установки или удаления уровней (или версий) протокола SSH. Могут быть установлены либо SSH1 (1), либо SSH2 (2), либо SSH 1 и SSH 2 одновременно.

По умолчанию 2

Формат ip ssh protocol [1] [2]

Режим Global Config

ip ssh server enable

Данная команда включает IP-сервер SSH. Новые SSH-соединения не разрешаются, но существующие продолжают работать до прекращения сессии пользователем или по таймауту.

По умолчанию включен

Формат ip ssh server enable

Режим Global Config

no ip ssh server enable

Данная команда отключает IP-сервер SSH.

Формат no ip ssh server enable

Режим Global Config

sshcon maxsessions

Эта команда указывает максимально возможное количество сессий SSH, которые могут быть установлены одновременно. Значение 0 указывает, что ssh-соединение не может быть установлено. Диапазон - от 0 до 5.

По умолчанию 5

Формат sshcon maxsessions 0-5

Режим Global Config

no sshcon maxsessions

Эта команда сбрасывает максимально возможное количество сессий SSH на заводские значения.

Формат no sshcon maxsessions

Режим Global Config

sshcon timeout

Эта команда устанавливает таймаут SSH-сессии, в минутах. Сессия остаётся активной до тех пор, пока время неактивности не достигнет указанного значения. Таймаут указывается десятичным числом в диапазоне 1 – 160.

Изменение времени сессии вступит в силу только для новых соединений. Каждая нажатая клавиша заново начинает отсчёт таймаута.

По умолчанию 5
Формат sshcon timeout *1-160*
Режим Global Config

no sshcon timeout

Эта команда сбрасывает значение таймаута SSH-сессии на заводские установки.

Изменение времени сессии вступит в силу только для новых соединений. Каждая нажатая клавиша заново начинает отсчёт таймаута.

Формат no sshcon timeout
Режим Global Config

show ip ssh

Эта команда показывает настройки ssh.

Формат show ip ssh
Режим Privileged EXEC

Термин	Значение
Administrative Mode	Это поле указывает, включен или отключен административно режим SSH.
Protocol Level	Версия протокола: 1, 2 либо 1 и 2.
SSH Sessions Currently Active	Количество текущих активных сеансов SSH.
Max SSH Sessions Allowed	Максимальное количество разрешенных сеансов SSH.
SSH Timeout	Значение таймаута SSH, в минутах.
Keys Present	Указывает, присутствуют ли на устройстве ключи SSH RSA и DSA.
Key Generation in Progress	Указывает на то, что генерация ключей RSA или DSA происходит в настоящий момент.

5.5. Команды безопасности управления

В этом разделе описаны команды, используемые для генерации ключей и сертификатов.

crypto certificate generate

Используйте эту команду, чтобы создать самоподписанный сертификат для HTTPS. Сгенерированный ключ RSA для SSL имеет длину 1024 бит. Полученный сертификат генерируется с именем, совпадающим с IP-адресом с наименьшим числовым значением на устройстве, и с продолжительностью 365 дней.

Формат crypto certificate generate

Режим Global Config

no crypto certificate generate

Данная команда удаляет сертификаты HTTPS с устройства, как загруженные, так и самоподписанные.

Формат no crypto certificate generate

Режим Global Config

crypto key generate rsa

Используйте эту команду, чтобы сгенерировать пару ключей RSA для SSH. Новые файлы ключей заменит все существующие или загруженные ключи RSA.

Формат crypto certificate generate rsa

Режим Global Config

no crypto key generate rsa

Данная команда используется для удаления файлов ключа RSA из устройства.

Формат no crypto key generate rsa

Режим Global Config

crypto key generate dsa

Используйте эту команду, чтобы сгенерировать пару ключей DSA для SSH. Новые файлы ключей заменит все существующие или загруженные ключи DSA.

Формат crypto certificate generate dsa

Режим Global Config

no crypto key generate dsa

Данная команда используется для удаления файлов ключа DSA из устройства.

Формат no crypto key generate dsa

Режим Global Config

5.6. Команды HTTP

В этом разделе описаны команды, которые используются для конфигурации доступа к коммутатору по протоколам HTTP и secure HTTP. Доступ к коммутатору через Веб-интерфейс включен по умолчанию. Большая часть того, что вы можете просмотреть и настроить с помощью командной строки, также доступно через Веб.

ip http accounting exec, ip https accounting exec

Данная команда применяет правила списка учета user exec accounting (только для начала и конца сессии) к HTTP и HTTPS.

ПРИМЕЧАНИЕ: Список учета user exec accounting должен быть создан с использованием команды “aaa accounting

”.

Формат ip {http|https} accounting exec {default|*listname*}

Режим Global Config

Параметры	Описание
http/https	Метод доступа к которому должен применяться список учета.
По умолчанию	Включение метода учета по умолчанию
listname	Цифро-буквенная строка содержащая имя списка метдов учета.

no ip http/https accounting exec

Эта команда удаляет список методов учета.

Формат no ip {http|https} accounting exec {default|*listname*}

Режим Global Config

ip http authentication

Используйте эту команду для указания методов аутентификации для пользователей http-сервера. Конфигурация по умолчанию - локальная база данных пользователей. Это действие имеет тот же эффект, что и команда ip http authentication local.

Дополнительные методы аутентификации используются только в том случае, если предыдущий метод возвращает ошибку (не в том случае, если аутентификация не проходит). Укажите none в командной строке в качестве окончательного метода, чтобы аутентификация проходила успешно даже в том случае, если все методы возвращают ошибку. Например, если none указано как метод аутентификации после radius, то в случае отказа RADIUS-сервера пользователи будут заходить без аутентификации.

По умолчанию local

Формат ip http authentication method1 *[*method2...*]*

Режим Global Config

Параметр	Описание
local	Используется локальная база данных пользователей.
none	Без аутентификации.
radius	Для аутентификации используется список серверов RADIUS.

Параметр	Описание
tacacs	Для аутентификации используется список серверов TACACS+.

ПРИМЕР: Следующий пример иллюстрирует настройку аутентификации http.

```
(switch)(config)# ip http authentication radius local
```

no ip http authentication

Данная команда возвращает заводские значения.

Формат no ip http authentication

Режим Global Config

ip https authentication

Используйте эту команду для указания методов аутентификации для пользователей https-сервера. Конфигурация по умолчанию - локальная база данных пользователей. Это действие имеет тот же эффект, что и команда **ip https authentication local**. Дополнительные методы аутентификации используются только в том случае, если предыдущий метод возвращает ошибку (не в том случае, если аутентификация не проходит). Укажите none в командной строке в качестве окончательного метода, чтобы аутентификация проходила успешно даже в том случае, если все методы возвращают ошибку. Например, если none указано как метод аутентификации после radius, то в случае отказа RADIUS-сервера пользователи будут заходить без аутентификации.

По умолчанию local

Формат ip https authentication method1 *[*method2...*]*

Режим Global Config

Параметр	Описание
local	Используется локальная база данных пользователей.
none	Без аутентификации.
radius	Для аутентификации используется список серверов RADIUS.
tacacs	Для аутентификации используется список серверов TACACS+.

ПРИМЕР: Следующий пример иллюстрирует настройку аутентификации https.

```
(switch)(config)# ip https authentication radius local
```

no ip https authentication

Данная команда возвращает заводские значения.

Формат no ip https authentication

Режим Global Config

ip http server

Данная команда позволяет получить доступ к коммутатору через Веб-интерфейс. Включенная опция позволяет пользователю авторизоваться на коммутаторе через Веб-интерфейс. Отключенная опция, соответственно, лишает пользователя такой возможности. Отключение Веб-интерфейса вступает в силу немедленно. Действие команды распространяется на все интерфейсы.

По умолчанию включен

Формат ip http server

Режим Global Config

no ip http server

Данная команда отключает доступ к коммутатору через Веб-интерфейс. Когда опция отключена, пользователь не может авторизоваться на коммутаторе через Веб-сервер.

Формат no ip http server

Режим Global Config

ip http secure-server

Данная команда включает защищенный сокет для безопасного HTTP.

По умолчанию disabled

Формат ip http secure-server

Режим Global Config

no ip http secure-server

Данная команда отключает защищенный сокет для безопасного HTTP.

Формат no ip http secure-server

Режим Global Config

ip http java

Данная команда включает Java режим Web. Режим Java применяется как к безопасным, так и обычным Веб-соединениям.

По умолчанию Enabled

Формат ip http java

Режим Global Config

no ip http java

Данная команда отключает Java режим Web. Режим Java применяется как к безопасным, так и обычным Веб-соединениям.

Формат no ip http java

Режим Global Config

ip http session hard-timeout

Данная команда настраивает жесткий таймаут для небезопасных HTTP-сессий, в часах. Нулевое значение вызывает бесконечный жесткий таймаут. При наступлении таймаута пользователю будет необходимо повторно пройти авторизацию. Время отсчитывается от начала сессии и не зависит от наличия или отсутствия активности.

По умолчанию 24

Формат ip http session hard-timeout 1-168

Режим Global Config

no ip http session hard-timeout

Данная команда возвращает заводские значения жесткого таймаута для небезопасных HTTP-сессий.

Формат no ip http session hard-timeout

Режим Global Config

ip http session maxsessions

Эта команда ограничивает количество допустимых небезопасных HTTP-сессий. Минимально допустимое значение равно нулю.

По умолчанию 16

Формат ip http session maxsessions *0-16*

Режим Global Config

no ip http session maxsessions

Данная команда возвращает заводские значения максимального количества допустимых небезопасных HTTP-сессий.

Формат no ip http session maxsessions

Режим Global Config

ip http session soft-timeout

Данная команда настраивает мягкий таймаут для небезопасных HTTP-сессий, в минутах. Нулевое значение вызывает бесконечный мягкий таймаут. При наступлении таймаута пользователю будет необходимо повторно пройти авторизацию. Время отсчитывается от начала сессии. Каждое обращение к коммутатору сбрасывает отсчет времени и начинает его заново.

По умолчанию 5

Формат ip http session soft-timeout *1-60*

Режим Global Config

no ip http session soft-timeout

Данная команда возвращает заводские значения мягкого таймаута для небезопасных HTTP-сессий.

Формат no ip http session soft-timeout

Режим Global Config

ip http secure-session hard-timeout

Данная команда настраивает жесткий таймаут для безопасных HTTP-сессий, в часах. При наступлении таймаута пользователю будет необходимо повторно пройти авторизацию. Время отсчитывается от начала сессии и не зависит от наличия или отсутствия активности. Нулевое значение недопустимо.

По умолчанию 24

Формат ip http secure-session hard-timeout *1-168*

Режим Global Config

no ip http secure-session hard-timeout

Данная команда возвращает заводские значения мягкого таймаута для безопасных HTTP-сессий.

Формат no ip http secure-session hard-timeout

Режим Global Config

ip http secure-session maxsessions

Эта команда ограничивает количество допустимых безопасных HTTP-сессий. Минимально допустимое значение равно нулю.

По умолчанию 16

Формат ip http secure-session maxsessions *0-16*

Режим Global Config

no ip http secure-session maxsessions

Данная команда возвращает заводские значения максимального количества допустимых безопасных HTTP-сессий.

Формат no ip http secure-session maxsessions

Режим Global Config

ip http secure-session soft-timeout

Данная команда настраивает мягкий таймаут для безопасных HTTP-сессий, в минутах. Нулевое значение вызывает бесконечный мягкий таймаут. При наступлении таймаута пользователю будет необходимо повторно пройти авторизацию. Время отсчитывается от начала сессии. Каждое обращение к коммутатору сбрасывает отсчет времени и начинает его заново. Нулевое значение недопустимо.

По умолчанию 5

Формат ip http secure-session soft-timeout *1-60*

Режим Global Config

no ip http secure-session soft-timeout

Данная команда возвращает заводские значения мягкого таймаута для небезопасных HTTP-сессий.

Формат no ip http secure-session soft-timeout

Режим Global Config

ip http secure-port

Эта команда используется для настройки порта SSL. Порт должен выбираться из диапазона 1025 – 65535. По умолчанию установлен порт 443.

По умолчанию 443

Формат ip http secure-port *portid*

Режим Global Config

no ip http secure-port

Данная команда сбрасывает номер порта SSL на заводские значения.

Формат no ip http secure-port

Режим Global Config

ip http secure-protocol

Эта команда используется для установки уровней протокола. Протокол может быть настроен как TLS, SSL3 или как TLS1 и SSL3.

По умолчанию SSL3 и TLS1.

Формат ip http secure-protocol *[SSL3] [TLS1]*

Режим Global Config

show ip http

Эта команда отображает параметры http.

Формат show ip http

Режим Privileged EXEC

Термин	Значение
HTTP Mode (Unsecure)	Небезопасный административный режим HTTP-сервера.
Java Mode	Административный режим Java, который применяется как к безопасным, так и небезопасным Веб-соединениям.
Maximum Allowable HTTP Sessions	Допустимое количество небезопасных HTTP-сессий.

Термин	Значение
HTTP Session Hard Timeout	Жесткий таймаут для небезопасных HTTP-сессий, в часах.
HTTP Session Soft Timeout	Мягкий таймаут для небезопасных HTTP-сессий, в минутах.
HTTP Mode (Secure)	Безопасный административный режим HTTP-сервера.
Термин	Значение
Secure Port	Номер порта безопасного HTTP-сервера.
Secure Protocol Level(s)	Уровень протокола может иметь значения: TLS, TSL1 , или SSL3 и TSL1.
Maximum Allowable HTTPS Sessions	Допустимое количество безопасных HTTP-сессий.
HTTPS Session Hard Timeout	Жесткий таймаут для безопасных HTTP-сессий, в часах.
Session Soft Timeout	Мягкий таймаут для безопасных HTTP-сессий, в минутах.
Certificate Present	Указывает, присутствуют ли на устройстве сертификаты защищённого сервера.
Certificate Generation in Progress	Указывает на то, генерируется ли сертификат в настоящее время.

5.7. Команды доступа

Используйте команды, описанные в этом разделе, для закрытия удаленного соединения или просмотра информации о подключениях к системе.

disconnect

Данная команда закрывает сессии HTTP, HTTPS и SSH. **all** - закрыть все сессии. Чтобы закрыть опеределенную сессию, введите ее **session-id**. Чтобы просмотреть возможные значения для **session-id**, используйте команду **show loginsession**.

Формат disconnect {*session_id* | all}

Режим Privileged EXEC

show loginsession

Данная команда отображает текущие подключения к коммутатору по протоколам Telnet и SSH, а также к консольному порту. Команда отображает сокращенные имена пользователей. Команда **show loginsession long** позволяет получать полные имена пользователей.

Формат show loginsession

Режим Privileged EXEC

Термин	Значение
ID	Идентификатор сессии
User Name	Имя пользователя, осуществившего вход в систему.
Connection From	IP-адрес компьютера клиента либо EIA-232 для консольного подключения.
Idle Time	Время неактивности данной сессии.
Session Time	Общее время существования сессии.
Session Type	Тип сессии: HTTP, HTTPS, Telnet, SSH или последовательный порт.

show loginsession long

Эта команда отображает полное имя пользователя, вошедшего в систему.

Формат show loginsession long

Режим Privileged EXEC

ПРИМЕР: Ниже приведен пример команды.

```
(switch) #show loginsession long
User Name
------
admin
test1111test1111test1111test1111test1111test1111test1111test1111
```

5.8. Команды учетных записей

В этом разделе описаны команды, используемые для добавления, управления и удаления пользователей системы. ПО коммутатора имеет двух пользователей по умолчанию: администратор (admin) и гость (guest). Администратор может просматривать и настраивать параметры системы, и гость может только просматривать.

ПРИМЕЧАНИЕ: Пользователя admin удалить невозможно. Может существовать только один пользователь с уровнем привилений 15. Можно настроить до 5 пользователей уровня 1.

aaa authentication login

Используйте эту команду для настройки аутентификации при входе в систему. Списки имен (по умолчанию и опциональный) создаются при помощи команды, используемой совместно с командой **aaa authentication login**. Создайте список, выполнив команду **aaa authentication login list-name method, где list-name** - это имя списка, которое может быть любой текстовой строкой. Аргумент **method** определяет перечень и порядок методов аутентификации, в заданной последовательности.

Дополнительные методы аутентификации используются только в том случае, если предыдущий метод возвращает ошибку (не в том случае, если аутентификация не проходит). Укажите none в командной строке в качестве окончательного метода, чтобы аутентификация проходила успешно даже в том случае, если все методы возвращают ошибку. Например, если none указано как метод аутентификации после radius, то в случае отказа RADIUS-сервера пользователи будут заходить без аутентификации.

По умолчанию defaultList. Используется консолью и содержит только метод «none».

networkList. Используется Telnet и SSH и содержит только метод «local».

Формат aaa authentication login {default | *list-name*} *method1 [method2...]*

Режим Global Config

Параметр	Значение
default	Использует перечисленные методы аутентификации, которые следуют за этим аргументом, в качестве списка методов по умолчанию при попытке пользователя войти в систему.
list-name	Имя списка методов аутентификации при входе пользователя в систему (текстовая строка до 15 символов).
method1... *[*method2...*]*	По крайней мере одно из следующих: enable. Использует пароль enable для проверки подлинности. • line. Использует пароль line для аутентификации. • local. Используется локальная база данных пользователей. • none. Без аутентификации. • radius. Для аутентификации используется список серверов RADIUS. • tacacs. Для аутентификации используется список серверов TACACS.

ПРИМЕР: Ниже приведен пример команды.

```
(switch)(config)# aaa authentication login default radius local enable none
```

no aaa authentication login

Данная команда возвращает заводские значения.

Формат aaa authentication login {default | *list-name*}

Режим Global Config

aaa authentication enable

Данная команда используется для настройки аутентификации для доступа к уровням с высокими привелегиями. enableList. - список по умолчанию. Он используется консолью, и содержит такие методы как enable, за которым следует none.

Еще один список по умолчанию, enableNetList, используется по умолчанию для Telnet и SSH. Список содержит метод enable,за которым следует метод deny . По умолчанию пароль enable не настроен. Соответственно, по умолчанию пользователи Telnet и SSH не могут получить доступ к режиму Privileged EXEC. С другой стороны, с настройками по умолчанию пользователь консоли всегда входит в режим Privileged EXEC без ввода пароля.

Списки имен (по умолчанию и опциональный) создаются при помощи команды aaa **authentication enable**, используемой совместно с командой **enable authentication**. Создайте список, выполнив команду **aaa authentication enable list-name method**, где **list-name** - это название списка (любая текстовая строка). Аргумент **method** определяет перечень и порядок методов аутентификации в заданной последовательности.

Менеджер учетных записей возвращает ERROR (а не PASS или FAIL) в том случае, если пароль не настроен, после чего переходит к следующему по списку методу аутернтификации. Метод none означает, что аутентификация не требуется.

Система запросит пользовательский пароль лишь в том случае, если он требуется. Не требуют пароля следующие методы аутентификации:

1. **none**
2. **deny**
3. **enable (если не настроен пароль enable)**
4. **line (если не настроен пароль line)**

ПРИМЕР: Обратите внимание на пример ниже.

a) **aaa authentication enable default enable none**

b) **aaa authentication enable default line none**

c) **aaa authentication enable default enable radius none**

d) **aaa authentication enable default line tacacs none**

Примеры **a** и **b** не запрашивают пароль, однако, поскольку примеры **c** и **d** содержат radius и tacacs, пароль отображается.

Если в списке методов аутентификации присутствует только enable, и пароль enable не настроен, коммутатор не будет запрашивать имя пользователя. В таких случаях запрашивается только пароль. В списках авторизации и аутентификации коммутатор поддерживает методы настройки после локальных методов. Если пользователь отсутствует в локальных базах данных - пробуется следующий метод.

Дополнительные методы аутентификации используются только в том случае, если предыдущий метод возвращает ошибку (не в том случае, если аутентификация не проходит). Укажите none в командной строке в качестве окончательного метода, чтобы аутентификация проходила успешно даже в том случае, если все методы возвращают ошибку.

ПРИМЕЧАНИЕ: Запросы коммутатора серверу RADIUS включают в себя имя пользователя **$enabx$**, где x - это требуемый уровень привилегий. Для включения аутентификации enable на серверах RADIUS, добавьте пользователей **$enabx$**. Идентификатор пользователя отправляется на сервера TACACS+ для включения аутентификации.

По умолчанию default

Формат aaa authentication enable {default | *list-name*} *method1 [method2...]*

Режим Global Config

Параметр	Описание
default	Использует перечисленные методы аутентификации, которые следуют за этим аргументом в качестве списка методов по умолчанию, при использовании высших уровней привилегий.
list-name	Название списка активированных методов аутентификации в формате текстовой строки, при использовании высших уровней привилегий. Диапазон: 1 – 15 символов.
method1 *[method2...]*	По крайней мере один из следующих: • **deny**. Доступ запрещен. • **enable**. Использует пароль enable для проверки подлинности. • **line**. Использует пароль line для аутентификации. • **none**. Без аутентификации. • **radius**. Для аутентификации используется список серверов RADIUS. • **tacacs**. Для аутентификации используется список серверов TACACS+.

ПРИМЕР: Следующий пример иллюстрирует настройку аутентификации при доступе к высшим уровням привилегий.

```
(switch)(config)# aaa authentication enable default enable
```

no aaa authentication enable

Данная команда возвращает заводские значения.

Формат no aaa authentication enable {default | *list-name*}

Режим Global Config

aaa authorization

Данная команда используется для настройки списков методов авторизации команд и режимов exec. Список имеет название default либо задаваемое пользователем название list-name. Если для авторизации выбран метод tacacs, команды авторизации будут переданы на сервер TACACS+. Если для авторизации выбран метод none, авторизация

команд не производится. Для авторизации команд можно создать до пяти (включительно) списков методов авторизации.

ПРИМЕЧАНИЕ: Локальные методы не поддерживаются для авторизации команд. Авторизация с RADIUS будет работать только в том случае, если примененный метод аутентификации - также radius.

Авторизация команд

Если авторизация настроена для режима line, менеджер учетных записей отправляет информацию о введенных командах на сервер AAA. Сервер AAA подтверждает полученную команду и возвращает либо PASS, либо FAIL. Одобренные команды выполняются. Команды, не получившие подтверждения, соответственно, не выполняются, а пользователь получает сообщение об ошибке. Команды различных утилит (такие как tftp и ping, а также исходящие команды telnet) также должны пройти авторизацию. Применение скрипта рассматривается как одна команда и тоже нуждается в прохождении авторизации. Команды конфигурации при загрузке применяются отдельно и подобную проверку авторизации не проходят.

Сценарий использования по-командной авторизации следующий:

1. Настройка списка методов авторизации **aaa authorization commands listname tacacs radius none**
2. Применение списка к каналу доступа (консоль, telnet, SSH) **authorization commands listname**
3. Введенные пользователем команды приходят авторизацию при помощи серверов TACACS+ или RADIUS, в результате которой принимаются либо отклоняются.

Авторизация режимов Exec

Если авторизация режима exec настроена для режима line, пользователю может не потребоваться использовать команду enable для входа в режим Privileged EXEC. В случае, когда ответ авторизации указывает на достаточные привилегии для режима Privileged EXEC, пользователь попадает сразу в него, а не в режим User EXEC.

Сценарий использования авторизации режимов Exec следующий:

1. Настройка списка методов авторизации **aaa authorization exec listname method1 [method2....]**
2. Применение списка к каналу доступа (консоль, telnet, SSH) **authorization exec listname**
3. Когда пользователь входит в систему, в дополнение к аутентификации будет выполнена дополнительная авторизация, которая определит, имеет ли пользователь доступ к режиму Privileged EXEC.

Формат aaa authorization {commands|exec} {default|*list-name*} *method1*[*method2*]

Режим Global Config

Параметр	Описание
commands	Обеспечивает авторизацию для всех команд, выполняемых пользователем.

Параметр	Описание
exec	Обеспечивает авторизацию режимов exec.
default	Список методов для сервисов авторизации по умолчанию.
Параметр	Описание
list-name	Строка из букв и цифр, служащая названием списка методов авторизации.
method	Поддерживаются TACACS+, RADIUS, Local и none.

ПРИМЕР: Ниже приведен пример команды.

```
(Routing) #
(Routing) #configure
(Routing) (Config)#aaa authorization exec default  tacacs+ none
(Routing) (Config)#aaa authorization commands default tacacs+ none
```

no aaa authorization

Данная команда удаляет список методов авторизации.

Формат no aaa authorization {commands|exec} {default|*list-name*}

Режим Global Config

authorization commands

Эта команда применяет список методов авторизцации команд к методам доступа (консоль, telnet, SSH).

Формат authorization commands [default|*list-name*]

Режим Line console, Line telnet, Line SSH

Параметр	Описание
commands	Включает командную авторизацию для каждой попытки выполнить команду.

no authorization commands

Данная команда отключает авторизацию команд режима line config.

Формат no authorization {commands|exec}

Режим Line console, Line telnet, Line SSH

ПРИМЕР: Ниже приведен пример команды.

```
(Switching) (Config)#line console
(Switching) (Config-line)#authorization commands list2
```

```
(Switching) (Config-line)#
(Switching) (Config-line)#exit
(Switching) (Config)#
```

authorization exec

Данная команда применяет список методов авторизации команд к методу доступа таким образом, что пользователям может не требоваться использовать команду enable для входа в режим Privileged EXEC.

Формат authorization exec *list-name*

Режим Line console, Line telnet, Line SSH

Параметр	Описание
list-name	Список командных методов авторизации.

no authorization exec

Данная команда удаляет командную авторизацию из режима line config.

Формат no authorization exec

Режим Line console, Line telnet, Line SSH

authorization exec default

Данная команда применяет список методов авторизации команд по умолчанию к методу доступа таким образом, что пользователям может не потребоваться использовать команду enable для входа в режим Privileged EXEC.

Формат authorization exec default

Режим Line console, Line telnet, Line SSH

show authorization methods

Данная команда отображает настроенные списки методов авторизации.

Формат show authorization methods

Режим Privileged EXEC

ПРИМЕР: Вывод командной строки для данной команды.

```
(Switching) #show authorization methods

Command Authorization List          Method
-------------------------------------------------------------------
dfltCmdAuthList                     tacacs          none
list2                               none            ndefined
list4                               tacacs          ndefined
```

```
Line                    Command Method List
-------------------------------------------------------------------
Console                 dfltCmdAuthList
Telnet                  dfltCmdAuthList
SSH                     dfltCmdAuthList

Exec Authorization List                 Method
-------------------------------------------------------------------
dfltExecAuthList                        tacacs          none
list2                                   none            undefined
list4                                   tacacs          undefined
Line                                    Exec Method List
-------------------------------------------------------------------
Console                                 dfltExecAuthList
Telnet                                  dfltExecAuthList
SSH                                     dfltExecAuthList
```

enable authentication

Используйте эту команду для указания списка методов аутентификации при доступе на уровень с более высокими привилегиями при удаленном подключении Telnet или консоли.

Формат enable authentication {default | *list-name*}

Режим line Config

Параметр	Описание
default	Использует список по умолчанию, созданный при помощи команды **aaa authentication enable**.
list-name	Использует пользовательский список, созданный командой **aaa authentication enable**.

ПРИМЕР: В следующем примере указывается метод аутентификации по умолчанию при доступе к высшим уровням привилегий через консоль.

```
(switch)(config)# line console
(switch)(config-line)# enable authentication default
```

no enable authentication

Используйте эту команду, чтобы вернуться к значениям по умолчанию, указанными командой enable authentication.

Формат no enable authentication

Режим line Config

username (Global Config)

Используйте команду **username** в режиме Global Config для добавления нового пользователя к локальной пользовательской базе данных. Уровень привилегий по умолчанию - 1. Ключевое слово encrypted позволяет администратору переносить локальные пользовательские пароли между устройствами без знания самих паролей. Если параметр **password** используется с параметром encrypted , пароль должен состоять из 128 шестнадцатеричных символов (не больше и не меньше). Если включена функция password strength, команда проверит стойкость пароля, и в случае несовпадения пароля с критериями выдаст ошибку. Опциональный параметр **override-complexity-check** отключает проверку надежности пароля.

Формат username *name* {password *password* [encrypted [override-complexity-check] | level *level* [encrypted [override-complexity-check]] | override-complexity-check]} | {level *level* [override-complexity-check] password}

Режим Global Config

Параметр	Описание
name	Имя пользователя. Диапазон: 1 – 64 символа.
password	Пароль пользователя. Диапазон 8 – 64 символа. Если выполнена команда **no passwords min-length**, значение может быть нулевым. Спецсимволы,которые разрешено использовать при создании пароля, включают в себя: ! # $ % & ' ( ) * + , - . / : ; < = > @ [\ ] ^ _ ` { | } ~.
level	Уровень пользователя. Уровень 0 может быть назначен пользователем с уровнем 15, чтобы временно приостановить доступ для этого пользователя. Диапазон 0 – 15. Введите уровень доступа 1 для непривилегированного доступа (приглашение switch>) и 15 - для привилегированного (приглашение switch#). Если уровень не задан, то принимается значение 1.
encrypted	Введен зашифрованный пароль, скопированный из конфигурации другого коммутатора.
override-complexity-check	Отключение проверки надежности паролей.

ПРИМЕР: Следующий пример иллюстрирует настройку пользователя bob с паролем xxxyyymmmm и уровнем 15.

```
(switch)(config)# username bob password xxxyyymmmm level 15
```

ПРИМЕР: Следующий пример иллюстрирует настройку пользователя test с паролем test и уровнем 1. Стойкость пароля не проверяется.

```
(switch)(config)# username test password testPassword level 1 override-complexity-check
```

ПРИМЕР: Третий пример.

```
(Switching) (Config)#username test password testtest
```

ПРИМЕР: Четвертый пример.

```
(Switching) (Config)# username test password
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafbf23b528d348cd
ba1b1b7ab91be4 2278e5e970dbfc62d16dcd13c0b864 level 1 encrypted override-complexity-
check
(Switching) (Config)# username test level 15 password
Enter new password:********
Confirm new password:********
```

ПРИМЕР: Пятый пример.

```
(Switching) (Config)# username test level 15 override-complexity-check password
Enter new password:********
Confirm new password:********
```

no username

Данная команда удаляет имя пользователя.

Формат no username *name*

Режим Global Config

username nopassword

Данная команда удаляет пароль существующего пользователя.

Формат username *name* nopassword *[level level]*

Режим Global Config

Параметр	Описание
name	Имя пользователя. Диапазон: 1 – 32 символа.
password	Пароль пользователя. Диапазон 8 – 64 символа.
level	Уровень пользователя. Уровень 0 может быть назначен пользователем с уровнем 15, чтобы временно приостановить доступ для этого пользователя. Диапазон 0 – 15.

username unlock

Данная команда разблокирует пользователя, заблокированного ранее. Только пользователь с уровнем доступа 15 может повторно активировать заблокированный аккаунт.

Формат username *name* unlock

Режим Global Config

show users

Эта команда отображает настроенные имена пользователей и их настройки. Команда show users показывает сокращенные имена пользователей. Чтобы увидеть полные имена пользователей, воспользуйтесь командой show users long. Команда show users доступна только для пользователей с уровнем 15.

Формат show users

Режим Privileged EXEC

Термин	Значение
User Name	Имя пользователя (для последовательного порта, Telnet или Веб-интерфейса).
Access Mode	Показывает, может ли пользователь вносить изменения в параметры коммутатора (уровень 15) или только просматривать текущие параметры (уровень 1). По умолчанию пользователь “admin имеет уровень 15 и пользователь “guest” имеет уровень 1.

show users long

Данная команда отображает полные имена пользователей коммутатора.

Формат show users long

Режим Privileged EXEC

ПРИМЕР: Ниже приведен пример команды.

```
(switch) #show users long
User Name
-----------
admin guest
test1111test1111test1111test1111
```

show users accounts

Эта команда отображает локальный статус пользователя в контексте блокировки аккаунта и устаревания пароля. Эта команда отображает сокращенные имена пользователей. Чтобы увидеть полные имена пользователей, воспользуйтесь командой show users long.

Формат show users accounts [detail]

Режим Privileged EXEC

Термин	Значение
User Name	Имя пользователя (локальное)
Access Level	Уровень доступа: 1 для непривилегированного доступа (приглашение switch>) и 15 - для привилегированного (приглашение switch#).
Password Aging	Количество дней с момента создания пароля, до тех пор пока пароль не утратит силу в связи с истечением срока действия.
Password Expiry Date	Дата устаревания текущего пароля
Lockout	Указывает, заблокирован ли аккаунт пользователя или нет (true or false).

Использование ключевого слова detail позволяет получить дополнительную информацию.

Термин	Значение
Password Override Complexity Check	Отображает результат проверки надежности пароля. Отключено по умолчанию.
Password Strength	Отображает надежность пароля (Strong или Weak). Это поле отображается только в том случае, если включена функция Password Strength.

ПРИМЕР: Следующий пример выводит информацию о локальной базе данных пользователей.

```
(switch)#show users accounts

UserName        Privilege   Password Aging   Password Expiry date   Lockout
-------------------------------------------------------------------------------
admin           15          ---             ---                    False
guest           1           ---             ---                    False

False console#show users accounts detail

UserName.....admin
Privilege .....15
Password Aging.....---
```

Password Expiry.....---
Lockout.....False
Override Complexity Check.....Disable Password
Strength.....---
UserName.....guest
Privilege 1
Password Aging.....---
Password Expiry.....---
Lockout.....False
Override Complexity Check.....Disable Password
Strength.....---

show users login-history [long]

Данная команда отображает информацию об истории входов пользователей в систему.

Формат show users login-history [long]

Режим Privileged EXEC

show users login-history [username]

Данная команда отображает информацию об истории входов пользователей в систему.

Формат show users login-history [username *name*]

Режим Privileged EXEC

Параметр	Описание
name	Имя пользователя. Диапазон: 1 – 20 символов.

ПРИМЕР: В следующем примере показывает история входов в систему.

Console>show users login-history

Login Time	Username	Protocol	Location
Jan 19 2005 08:23:48	Bob	Serial	
Jan 19 2005 08:29:29	Robert	HTTP	172.16.0.8
Jan 19 2005 08:42:31	John	SSH	172.16.0.1
Jan 19 2005 08:49:52	Betty	Telnet	172.16.1.7

login authentication

Используйте эту команду для указания списка методов аутентификации для входа в систему через командную строку (консоль, telnet или SSH). В заводской конфигурации используется список по умолчанию, настроенный командой aaa authentication login.

Формат login authentication {default | *list-name*}

Режим Line Configuration

Параметр	Описание
default	Использует список по умолчанию, созданный при помощи команды **aaa authentication login**.
list-name	Использует пользовательский список, созданный командой **aaa authentication login**.

ПРИМЕР: В следующем примере показана настройка метода аутентификации по умолчанию при доступе через консоль.

```
(switch) (config)# line console
(switch) (config-line)# login authentication default
```

no login authentication

Используйте эту команду, чтобы вернуться к значениям по умолчанию, указанными командой **authentication login**.

password

Данная команда позволяет пользователю, вошедшему в систему, поменять пароль не имея привилегий уровня 15.

Формат password *cr*

Режим User EXEC

ПРИМЕР: Ниже приведен пример команды. **console>password**

```
Enter old password:********
Enter new password:********
Confirm new password:********
```

password (Line Configuration)

Команда password в режиме Line Configuration задаёт пароль режима line. По умолчанию пароль не задан.

Формат password [*password* [encrypted]]

Режим line Config

Параметр	Значение
password	Пароль для этого уровня. Диапазон: 8 – 64 символа

Параметр	Значение
encrypted	Зашифрованный пароль, скопированный из конфигурации другого коммутатора. Зашифрованный пароль должен быть 128 символов, поскольку предполагается что этот пароль уже зашифрован с помощью алгоритма AES.

ПРИМЕР: Следующий пример иллюстрирует настройку пароля mcmxxyyy режима line

```
(switch)(config-line)# password mcmxxyyy
```

ПРИМЕР: Ниже приведен еще один пример команды.

```
(Switching)(Config-line)# password testtest
(Switching) (Config-line)# password
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafbf23b528d348cd
ba1b1b7ab91be4 2278e5e970dbfc62d16dcd13c0b864 encrypted
(Switching) (Config-line)# password
Enter new password:********
Confirm new password:********
```

no password (Line Configuration)

Данная команда удаляет пароль режима line.

Формат no password

Режим Line Config

password (User EXEC)

Данная команда позволяет пользователю поменять свой пароль. Она должна использоваться после устаревания текущего пароля. Система требует ввести сначала старый пароль, а затем новый.

Формат password

Режим User EXEC

ПРИМЕР: Следующий пример иллюстрирует последовательность запросов при смене пароля.

```
(switch)>password
Enter old password:********
Enter new password:********
Confirm new password:********
```

password (aaa IAS User Config)

Данная команда используется для настройки пароля пользователя. Дополнительный параметр [encrypted] используется для указания на то, что пароль уже предоставляется в зашифрованной форме.

Формат password *password* [encrypted]

Режим aaa IAS User Config

no password (aaa IAS User Config)

Данная команда используется для очистки пароля пользователя.

Формат no password

Режим aaa IAS User Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) #
(Routing) #configure
(Routing) (Config)#aaa ias-user username client-1
(Routing) (Config-aaa-ias-User)#password client123
(Routing) (Config-aaa-ias-User)#no password
```

ПРИМЕР: Пример добавления клиента MAB во внутреннюю базу данных пользователей.

```
(Routing) #
(Routing) #configure
(Routing) (Config)#aaa ias-user username 1f3ccb1157
(Routing) (Config-aaa-ias-User)#password 1f3ccb1157
(Routing) (Config-aaa-ias-User)#exit
(Routing) (Config)#
```

enable password (Privileged EXEC)

Используйте команду enable password для установки локального пароля, защищающего доступ в режим privileged EXEC.

Формат enable password [*password* [encrypted]]

Режим Global Config

Параметр	Описание
password	Строка пароля. Диапазон: 8 – 64 символа.
encrypted	Введен зашифрованный пароль, скопированный из конфигурации другого коммутатора. Зашифрованный пароль должен состоять из 128 символов, поскольку предполагается, что этот пароль уже зашифрован с помощью алгоритма AES.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Switching) #enable password testtest
(Switching) #enable password
```

e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafbf23b528d348cd ba1b1b7ab91be4 2278e5e970dbfc62d16dcd13c0b864 encrypted

(Switching) #enable password

Enter old password:********

Enter new password:********

Confirm new password:********

no enable password (Privileged EXEC)

Данная команда отменяет требование пароля.

Формат no enable password

Режим Global Config

passwords min-length

Используйте эту команду для настройки минимальной длины пароля для локальных пользователей. Значение применяется также к паролям enable. Диапазон: 8 – 64.

По умолчанию 8

Формат passwords min-length *8-64*

Режим Global Config

no passwords min-length

Используйте эту команду для сброса значения минимальной длины пароля на заводские настройки.

Формат no passwords min-length

Режим Global Config

passwords history

Данная команда задает количество предыдущих паролей, которые должны храниться в системе для каждой учетной записи. Когда локальный пользователь изменяет свой пароль, система не позволит использовать пароли, уже бывшие в употреблении. Это гарантирует, что пользователи не будут использовать свои пароли повторно слишком часто. Диапазон: 0 – 10.

По умолчанию 0

Формат passwords history *0-10*

Режим Global Config

no passwords history

Данная команда сбрасывает количество предыдущих паролей, которые должны храниться в системе, на заводские значения.

Формат no passwords history

Режим Global Config

passwords aging

Данная команда настраивает срок устаревания паролей для локальных пользователей. Как только срок истекает, пользователь будет должен ввести изменить пароль перед следующим входом в систему. Диапазон: 1 – 365. Значение по умолчанию - 0 (пароль не устаревает никогда).

По умолчанию 0

Формат passwords aging *1-365*

Режим Global Config

no passwords aging

Данная команда сбрасывает срок устаревания паролей на заводские значения.

Формат no passwords aging

Режим Global Config

passwords lock-out

Данная команда используется для блокировки учетных записей, которые не смогли войти в систему из-за неправильного ввода паролей. Как только счётчик неправильных попыток включается, пользователь должен вводить правильный пароль за определенное количество попыток. В противном случае, пользователю будет отказано в авторизации. Только пользователь с уровнем доступа 15 может повторно активировать заблокированный аккаунт. Блокировка из-за превышения количества попыток не распространяется на попытки входа через последовательный консольный порт. Диапазон: 1 – 15. Значение по умолчанию - 0 (счетчик неправильных попыток не задействуется).

По умолчанию 0

Формат passwords lock-out *1-5*

Режим Global Config

no passwords lock-out

Данная команда сбрасывает настройки блокировки по причине ввода неверного пароля на заводские значения.

Формат no passwords lock-out

Режим Global Config

passwords strength-check

Данная команда включает функцию проверки надежности пароля. Она используется для проверки стойкости вводимого пароля к возможным попыткам взлома.

По умолчанию disabled

Формат passwords strength-check

Режим Global Config

no passwords strength-check

Данная команда сбрасывает настройки функции проверки надежности паролей на заводские значения.

Формат no passwords strength-check

Режим Global Config

passwords strength maximum consecutive-characters

Данная команда настраивает максимальное разрешенное количество использования следующих друг за другом символов при создании пароля. Диапазон: 0 – 15. Значение по умолчанию - 0. Значение 0 означает, что ограничения на количество следующих друг за другом символов в пароле полностью сняты.

По умолчанию 0

Формат passwords strength maximum consecutive-characters *0-15*

Режим Global Config

passwords strength maximum repeated-characters

Данная команда настраивает максимальное разрешенное количество использования одного и того же символа несколько раз подряд при создании пароля. Диапазон: 0 – 15. Значение по умолчанию - 0. Значение 0 означает, что ограничения на количество одинаковых последовательных символов в пароле полностью сняты.

По умолчанию 0

Формат passwords strength maximum repeated-characters *0-15*

Режим Global Config

passwords strength minimum uppercase-letters

Данная команда устанавливает минимальное количество прописных символов (в верхнем регистре), которые должны содержаться в пароле. Диапазон: 0 – 16. Значение по умолчанию - 2. Значение 0 снимает ограничение.

По умолчанию 2

Формат passwords strength minimum uppercase-letters

Режим Global Config

no passwords strength minimum uppercase-letters

Данная команда сбрасывает минимально достаточное количество прописных символов в пароле до заводских значений.

Формат no passwords minimum uppercase-letter

Режим Global Config

passwords strength minimum lowercase-letters

Данная команда устанавливает минимальное количество строчных символов (в нижнем регистре), которые должны содержаться в пароле. Диапазон: 0 – 16. Значение по умолчанию - 2. Значение 0 снимает ограничение.

По умолчанию 2

Формат passwords strength minimum lowercase-letters

Режим Global Config

no passwords strength minimum lowercase-letters

Данная команда сбрасывает минимально достаточное количество строчных символов в пароле до заводских значений.

Формат no passwords minimum lowercase-letter

Режим Global Config

passwords strength minimum numeric-characters

Данная команда устанавливает минимальное количество цифр, которые должны содержаться в пароле. Диапазон: 0 – 16. Значение по умолчанию - 2. Значение 0 снимает ограничение.

По умолчанию 2

Формат passwords strength minimum numeric-characters

Режим Global Config

no passwords strength minimum numeric-characters

Данная команда сбрасывает минимально достаточное количество цифр в пароле до заводских значений.

Формат no passwords minimum numeric-letter

Режим Global Config

passwords strength minimum special-characters

Данная команда устанавливает минимальное количество спецсимволов, которые должны содержаться в пароле. Диапазон: 0 – 16. Значение по умолчанию - 2. Значение 0 снимает ограничение.

По умолчанию 2

Формат passwords strength minimum special-characters

Режим Global Config

no passwords strength minimum special-characters

Данная команда сбрасывает минимально достаточное количество спецсимволов в пароле до заводских значений.

Формат no passwords minimum special-letter

Режим Global Config

passwords strength minimum character-classes

Данная команда устанавливает минимальное количество разных классов символов, которые должны содержаться в пароле. Существует 4 класса: прописные и строчные буквы, цифры и спецсимволы. Диапазон: 0 – 4. Значение по умолчанию - 4.

По умолчанию 4

Формат passwords strength minimum character-classes

Режим Global Config

no passwords strength minimum character-classes

Данная команда сбрасывает минимально достаточное количество разных классов символов в пароле до заводских значений.

Формат no passwords minimum character-classes

Режим Global Config

passwords strength exclude-keyword

Данная команда исключает определенные ключевые слова при настройке пароля. Ключевые слова в любой форме (между частями строки, в разном регистре, в обратном напрпавлении) не принимаются в качестве подстроки. Пользователи могут настраивать до 3 ключевых слов.

Формат passwords strength exclude-keyword *keyword*

Режим Global Config

no passwords strength exclude-keyword

Данная команда снимает ограничения на использование ключевых слов и очищает ранее настроенный список слов.

Формат no passwords exclude-keyword *[keyword]*

Режим Global Config

show passwords configuration

Данная команда отображает текущие настройки управления паролями.

Формат show passwords configuration

Режим Privileged EXEC

Термин	Значение
Minimum Password Length	Минимальное количество символов, требуемое при изменении паролей.
Password History	Количество паролей, хранимых в памяти для защиты от повторного использования одних и тех же паролей.
Password Aging	Срок, в течение которого пароль останется действительным.

Термин	Значение
Lockout Attempts	Количество неудачных попыток входа в систему до блокировки.
Minimum Password Uppercase Letters	Минимальное количество прописных букв, требуемое при создании пароля.
Minimum Password Lowercase Letters	Минимальное количество строчных букв, требуемое при создании пароля.
Minimum Password Numeric Characters	Минимальное количество цифр, требуемое при создании паролей.
Maximum Password Consecutive Characters	Максимальное количество символов, идущих подряд, разрешенное для использования при создании пароля.
Maximum Password Repeated Characters	Максимальное количество повторения символа, разрешенное при создании пароля.
Minimum Password Character Classes	Минимальное количество классов символов (прописные буквы, строчные буквы, цифры и спецсимволы), необходимое при создании пароля.
Password ExcludeKeywords	Набор ключевых слов, которые будут исключены из настроенного пароля при проверке надежности.

show passwords result

Данная команда отображает информацию о результатах последней установки пароля.

Формат show passwords result

Режим Privileged EXEC

Термин	Значение
Last User Whose Password Is Set	Показывает имя последнего пользователя, настраивавшего свой пароль.
Password Strength Check	Показывает, включена ли функция проверки надежности пароля.
Last Password Set Result	Показывает, была ли успешной последняя попытка настройки пароля. Если попытка не удалась, указываются причины.

aaa ias-user username

Выделенная внутренняя база данных Внутреннего сервера аутентификации (Internal Authentication Server, или IAS) используется для локальной аутентификации пользователей сети посредством функции IEEE 802.1X.

Используйте команды aaa ias-user username в режиме Global Config для добавления определенного пользователя к внутренней базе данных. Данная команда также меняет режим на AAA User Config.

Формат aaa ias-user username *user*

Режим Global Config

no aaa ias-user username

Данная команда удаляет определенного пользователя из внутренней базы данных.

Формат no aaa ias-user username *user*

Режим Global Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) #
(Routing) #configure
(Routing) (Config)#aaa ias-user username client-1
(Routing) (Config-aaa-ias-User)#exit
(Routing) (Config)#no aaa ias-user username client-1 (Routing) (Config)#
```

aaa session-id

Используйте эту команду в режиме Global Config, чтобы определить, что тот же session-id используется для аутентификации, авторизации и учета (Authentication, Authorization and Accounting).

По умолчанию common

Формат aaa session-id [common | unique]

Режим Global Config

Параметр	Описание
common	Один и тот же session-id используется для всех сервисов типа AAA.
unique	Для всех сервисов типа AAA используется разный session-id.

no aaa session-id

Используйте эту команду в режиме Global Config для сброса поведения aaa session-id на установки по умолчанию.

Формат no aaa session-id [unique]

Режим Global Config

aaa accounting

Используйте эту команду в режиме Global Config, чтобы создать список методов учета пользовательских сессий режима EXEC, выполняемых пользователем команд либо DOT1X. Список может быть **default**, либо под пользовательским названием **list-name**. Записи учета, включенные для режима line, могут быть отправлены как при начале, так и при конце (**start-stop**), либо только в конце (**stop-only**) сессии. Если указано **none**, учет для данного списка отключается. Если для учета выбран метод **tacacs**, записи учета будут переданы на сервер TACACS+. Если для учета выбран метод **radius**, записи учета будут переданы на сервер RADIUS.

ПРИМЕЧАНИЕ: Обратите внимание на следующее:

- Для каждого типа exec и учета команд можно создать до пяти (включительно) списков методов учета.
- Для DOT1X может быть создан только список методов учета по умолчанию. Создание других списков для этого не предусмотрено.
- Одно и то же название списка может быть использовано для обоих типов учета: exec и учета команд.
- Учет AAA для команд не поддерживается с методом учета RADIUS.
- Поддерживаемые типы записей для учета DOT1X: Start-stop или None. Start-stop включает учёт, а None - отключает.
- RADIUS является единственным поддерживаемым типом учета для DOT1X.

Формат aaa accounting {exec | commands | dot1x} {default | list_name} {start-stop | stoponly |none} *method1* [*method2*…]

Режим Global Config

Параметр	Описание
exec	Обеспечивает учет для пользовательских терминальных сессий EXEC.

Параметр	Описание
commands	Обеспечивает учет для всех команд, выполняемых пользователем.
dot1x	Обеспечивает учет для пользовательских команд DOT1X.
default	Список методов для сервисов учета по умолчанию.
list-name	Строка из букв и цифр, служащая названием списка методов учета.
start-stop	Отправляет начальное уведомление об учете в начале процесса и конечное - в конце.
stop-only	Отправляет конечное уведомление об учете в конце пользовательского процесса.
none	Отключает службы учета на этой линии.
method	Использовать севрер TACACS или Radius для учета.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) #
(Routing) #configure
(Routing) #aaa accounting commands default stop-only tacacs
(Routing) #aaa accounting exec default start-stop radius
(Routing) #aaa accounting dot1x default start-stop radius
(Routing) #aaa accounting dot1x default none (Routing)
#exit
```

Для одинакового набора типов учета и имен списков администратор может изменить тип записи или список методов без необходимости сначала удалить предыдущую конфигурацию.

```
(Routing) #
(Routing) #configure
(Routing) #aaa accounting exec ExecList stop-only tacacs
(Routing) #aaa accounting exec ExecList start-stop tacacs
(Routing) #aaa accounting exec ExecList start-stop tacacs radius
```

Первая команда aaa создает список методов для сессий exec с именем ExecList, с типом записи record-type - stop-only и методом method - TACACS+. Вторая команда изменяет тип записи record type на start-stop вместо stop-only для того же списка методов. Третья команда для того же списка меняет список методов methods list на {tacacs,radius} вместо {tacacs}.

no aaa accounting

Данная команда удаляет список методов учета.

Формат no aaa accounting {exec | commands | dot1x} {default | list_name default}

Режим Global Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) #
(Routing) #configure
(Routing) #aaa accounting commands userCmdAudit stop-only tacacs radius
(Routing) #no aaa accounting commands userCmdAudit (Routing)
#exit
```

password (AAA IAS User Configuration)

Данная команда указывает пароль для пользователя базы данных IAS. Дополнительный параметр **encrypted** используется для указания на то, что пароль уже предоставляется в зашифрованной форме.

Формат password *password* [encrypted]

Режим AAA IAS User Config

Параметр	Значение
password	Пароль для этого уровня. Диапазон: 8 – 64 символа
encrypted	Зашифрованный пароль, скопированный из конфигурации другого коммутатора.

no password (AAA IAS User Configuration)

Данная команда удаляет пароль пользователя.

Формат no password

Режим AAA IAS User Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) #
(Routing) #configure
(Routing) (Config)#aaa ias-user username client-1
(Routing) (Config-aaa-ias-User)#password client123
(Routing) (Config-aaa-ias-User)#no password
```

ПРИМЕР: Пример добавления клиента MAB во внутреннюю базу данных пользователей.

```
(Routing) #
(Routing) #configure
(Routing) (Config)#aaa ias-user username 1f3ccb1157
```

```
(Routing) (Config-aaa-ias-User)#password 1f3ccb1157
(Routing) (Config-aaa-ias-User)#exit
(Routing) (Config)#
```

clear aaa ias-users

Данная команда удаляет всех пользователей из базы данных IAS.

Формат clear aaa ias-users

Режим Privileged EXEC

ПРИМЕР: Ниже приведен пример команды.

```
(Routing) #
(Routing) #clear aaa ias-users
(Routing) #
```

show aaa ias-users

Данная команда показывает настроенных пользователей IAS и их атрибуты. Пароли не отображаются.

Формат show aaa ias-users [username]

Режим Privileged EXEC

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) #
(Routing) #show aaa ias-users
UserName
------------------
Client-1
Client-2
```

ПРИМЕР: Команды конфигурации IAS, показанные в выводе команды «show running-config». Пароли, отображаемые в выводе команды, всегда зашифрованы.

```
aaa ias-user username client-1
password a45c74fdf50a558a2b5cf05573cd633bac2c6c598d54497ad4c46104918f2c encrypted
exit
```

accounting

Данная команда в режиме Line Configuration применяет список методов учета к режиму line config (консоль/telnet/ssh).

Формат accounting {exec | commands } {default | *listname*}

Режим Line Configuration

Параметр	Описание
exec	Включает учет для сессии EXEC.
commands	Включает учет для каждой попытки выполнить команду. Если пользователь включает учет для режима exec для текущего типа конфигурации, его сеанс будет прекращен.
default	Список учета по умолчанию.
listname	Название списка, не более 15 символов.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) #
(Routing) #configure
(Routing) (Config)#line telnet
(Routing)(Config-line)# accounting exec default (Routing) #exit
```

no accounting

Данная команда удаляет учет из режима Line Configuration.

Формат no accounting {exec|commands]

Режим Line Configuration

show accounting

Данная команда отображает методы списков учёта.

Формат show accounting

Режим Privileged EXEC

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show accounting
Number of Accounting Notifications sent at beginning of an EXEC session:                0
Errors when sending Accounting Notifications beginning of an EXEC session:              0
Number of Accounting Notifications at end of an EXEC session:                          0
Errors when sending Accounting Notifications at end of an EXEC session:                0
Number of Accounting Notifications sent at beginning of a command execution:           0
Errors when sending Accounting Notifications at beginning of a command execution:      0
Number of Accounting Notifications sent at end of a command execution:                 0
Errors when sending Accounting Notifications at end of a command execution:            0
```

show accounting methods

Данная команда отображает настроенные списки методов учета.

Формат show accounting methods

Режим Privileged EXEC

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #
(Routing) #show accounting methods
Acct Type          Method Name        Record Type      Method Type
-------------------------------------------------------------------
Exec               dfltExecList       start-stop       TACACS
Commands           dfltCmdsList       stop-only        TACACS
Commands           UserCmdAudit       start-stop       TACACS
DOT1X              dfltDot1xList      start-stop       radius

Line               EXEC Method List        Command Method List
-------------------------------------------------------------------
Console            dfltExecList            dfltCmdsList
Telnet             dfltExecList            dfltCmdsList
SSH                dfltExecList            UserCmdAudit
```

clear accounting statistics

Данная команда очищает статистику учета.

Формат clear accounting statistics

Режим Privileged EXEC

5.9. Команды SNMP

В этом разделе описаны команды, который используется для настройки доступа к коммутатору по протоколу SNMP. Коммутатор может быть настроен в качестве агента SNMP, чтобы осуществлять коммуникацию с SNMP-администраторами сети.

snmp-server

Эта команда устанавливает имя и местонахождение коммутатора и организацию, отвечающую за сеть. Параметры *name*, *loc* и *con* могут иметь длину до 255 символов.

По умолчанию none

Формат snmp-server {sysname *name* | location *loc* | contact *con*}

Режим Global Config

ПРИМЕЧАНИЕ: Для очистки snmp-сервера используйте пустую строку в кавычках. Например, snmp-server {sysname “ “} очищает системное имя.

snmp-server community

Данная команда создает новое SNMP-сообщество и называет его. Опционально указываются режим доступа, разрешенный IP-адрес и создается представление для сообщества.

ПРИМЕЧАНИЕ: Имя сообщества должно быть уникальным в пределах Таблицы Сообществ. При выполнении нескольких записей и использовании того же имени сообщества, хранится и обрабатывается только первая запись. Дублирующие записи игнорируются.

По умолчанию Создается два сообщества:

- public, с разрешениями только для чтения, именем представления Default, разрешающее доступ со всех IP-адресов.
- private, с разрешениями для чтения и записи, именем представления Default, разрешающее доступ со всех IP-адресов.

Формат snmp-server community *community-string* [{ro | rw |su *}*] [ipaddress *ip-address*] [view *view-name*]

Режим Global Config

Параметр	Описание
community-name	Имя, ассоциируемое с данным коммутатором и с набором SNMP-администраторов, управляющих со специальным уровнем привилегий. Длина *community-name* может быть до 16 символов (чувствительно к регистру).
ro | rw | su	Метод доступа SNMP-сообщества, который может быть: public (Read-Only/RO), private (Read-Write/RW) либо Super User (SU).
ip-address	Связанный с сообществом адрес отправки SNMP-пакета. Используется вместе со значением маски клиентского IP-адреса, и служит для обозначения диапазона IP-адресов, с которых клиенты SNMP могут использовать это сообщество для доступа к устройству. Значение 0.0.0.0 разрешает доступ с любого IP-адреса. В противном случае это значение равно AND с маской для определения диапазона допустимых IP-адресов клиента.
view-name	Имя представления для создания или обновления.

no snmp-server community

Данная команда удаляет определенное имя сообщества из таблицы. *name* - имя сообщества, которое следует удалить.

Формат no snmp-server community *community-name*

Режим Global Config

snmp-server community-group

Данная команда настраивает строку доступа сообщества access для получения доступа через протоколы SNMPv1 и SNMPv2c.

Формат snmp-server community-group *community-string group-name* [ipaddress *ipaddress*]

Режим Global Config

Параметр	Описание
communitystring	Сообщество, которое создано и ассоциируется с определенной группой. Диапазон - от 1 до 20 символов.
group-name	Имя группы, с которой ассоциируется сообщество. Диапазон - от 1 до 30 символов.
ipaddress	Опционально - адрес IPv4, с которого может осуществляться доступ к сообществу.

snmp-server enable traps violation

Компонент блокировки MAC на порту интерпретирует эту команду и настраивает отправку SNMP-trap в случае нарушения с частотой по умолчанию 30 секунд. Команда в Global режиме настраивает режим отправки trap на всех интерфейсах, для которых может быть применена защита портов. Глобального режима настройки отправки trap как такового не существует.

ПРИМЕЧАНИЕ: Другие команды защиты портов смотрите в разделе “Команды защищенных портов”.

По умолчанию disabled

Формат snmp-server enable traps violation

Режим Global Config
Interface Config

no snmp-server enable traps violation

Эта команда отключает отправку новых trap.

Формат no snmp-server enable traps violation

Режим Interface Config

snmp-server enable traps

Данная команда активирует Authentication Flag.

По умолчанию включен

Формат snmp-server enable traps

Режим Global Config

no snmp-server enable traps

Данная команда отключает Authentication Flag.

Формат no snmp-server enable traps

Режим Global Config

snmp-server port

Данная команда позволяет настроить UDP-порт, на котором SNMP-сервер будет слушать запросы.

По умолчанию 161

Формат snmp-server port *1025-65535*

Режим Global Config

no snmp-server port

Данная команда возвращает заводские значения номера UDP-порта, на котором SNMP-сервер будет слушать запросы.

Формат no snmp-server port

Режим Global Config

snmp trap link-status

Данная команда включает отправку trap о состоянии линка на интерфейсе либо на группе интерфейсов.

ПРИМЕЧАНИЕ: Данная команда работает лишь в том случае, если активирован Link Up/Down Flag.

Формат snmp trap link-status

Режим Interface Config

no snmp trap link-status

Данная команда отключает trap о состоянии линка.

ПРИМЕЧАНИЕ: Данная команда работает лишь в том случае, если активирован Link Up/Down Flag.

Формат no snmp trap link-status

Режим Interface Config

snmp trap link-status all

Данная команда включает отправку trap о состоянии линка на всех интерфейсах.

ПРИМЕЧАНИЕ: Данная команда работает лишь в том случае, если активирован Link Up/Down Flag.

Формат snmp trap link-status all

Режим Global Config

no snmp trap link-status all

Данная команда отключает отправку trap о состоянии линка на всех интерфейсах.

ПРИМЕЧАНИЕ: Данная команда работает лишь в том случае, если активирован Link Up/Down Flag.

Формат no snmp trap link-status all

Режим Global Config

snmp-server enable traps linkmode

ПРИМЕЧАНИЕ: Эта команда может быть доступна не на всех платформах.

Команда включает SNMP-trap Link Up/Downдля всего коммутатора. Когда эта функция включена, trap отправляются только если связанный с портом параметр Link Trap flag включен. См. “show snmp”.

По умолчанию включен

Формат snmp-server enable traps linkmode

Режим Global Config

no snmp-server enable traps linkmode

Команда отключает trap Link Up/Down для всего коммутатора.

Формат no snmp-server enable traps linkmode

Режим Global Config

snmp-server enable traps multiusers

Данная команда включает отправку trap Multiple User. Multiple User trap отправляется, когда пользователь входит в интерфейс терминала (EIA 232 или Telnet) при уже существующей сессии интерфейса терминала.

По умолчанию включен

Формат snmp-server enable traps multiusers

Режим Global Config

no snmp-server enable traps multiusers

Данная команда отключает Multiple User trap.

Формат no snmp-server enable traps multiusers

Режим Global Config

snmp-server enable traps stpmode

Данная команда активирует отправку trap о новом root коммутаторе и trap об изменении топологии.

По умолчанию включен

Формат snmp-server enable traps stpmode

Режим Global Config

no snmp-server enable traps stpmode

Данная команда отключает отправку trap о новом root коммутаторе и trap об изменении топологии.

Формат no snmp-server enable traps stpmode

Режим Global Config

snmp-server engineID local

Данная команда настраивает SNMP engine ID на локальном устройстве.

По умолчанию Engine ID настраивается автоматически на основе MAC-адреса устройства.

Формат snmp-server engineID local {*engineid-string*|default}

Режим Global Config

Параметр	Описание
engineid-string	Шестнадцатеричная строка, идентифицирующая engine-id, используемая для локализации конфигурации. Engine-id должен быть четной длины в диапазоне от 6 до 32 шестнадцатеричных символов.
default	Engine ID настраивается автоматически на основе MAC-адреса устройства.

ВНИМАНИЕ: ИЗМЕНЕНИЕ ENGINE-ID АННУЛИРУЕТ ВСЕ НАСТРОЙКИ SNMP.

no snmp-server engineID local

Команда удаляет указанный engine ID.

По умолчанию Engine ID настраивается автоматически на основе MAC-адреса устройства.

Формат no snmp-server engineID local

Режим Global Config

snmp-server filter

Данная команда создает запись фильтра для ограничения типа trap, отправляемых на хост.

По умолчанию Фильтры не создаются.

Формат snmp-server filter *filtername oid-tree* {included|excluded}

Режим Global Config

Параметр	Описание
filtername	Создаётся название для фильтра. Диапазон - от 1 до 30 символов.

Параметр	Описание
oid-tree	Поддрево OID для включения в фильтр или исключение из него. Поддрева могут быть заданы численно (1.3.6.2.4) либо ключевым словом (system). Звездочки могут использоваться для определения семей поддрев (1.3.*.4).
included	Древо включено в фильтр.
excluded	Древо исключено из фильтра.

`no snmp-server filter`

Команда удаляет указанный фильтр.

По умолчанию Фильтры не создаются.

Формат snmp-server filter *filtername* [*oid-tree*]

Режим Global Config

`snmp-server group`

Данная команда создает группу доступа SNMP.

По умолчанию Общие группы создаются для всех версий и привилегий с использованием представлений по умолчанию.

Формат snmp-server group *group-name* {v1 | v2c | v3 {noauth | auth | priv}} [context *contextname*] [read *read-view*] [write *write-view*] [notify *notify-view*]

Режим Global Config

Параметр	Описание
group-name	Имя группы используемое при настройке сообществ и пользователей. Диапазон - от 1 до 30 символов.
v1	Эта группа может получить доступ только через протокол SNMPv1.
v2	Эта группа может получить доступ только через протокол SNMPv2c.
v3	Эта группа может получить доступ только через протокол SNMPv3.
noauth	Доступ к данной группе можно получить только в том случае, если аутентификация и шифрование не используются. Применяется только в случае выбора протокола SNMPv3.

Параметр	Описание
auth	Доступ к данной группе можно получить только в том случае, если используется аутентификация, но не шифрование . Применяется только в случае выбора протокола SNMPv3.
priv	Доступ к данной группе можно получить только в том случае, если используются и аутентификация, и шифрование. Применяется только в случае выбора протокола SNMPv3.
context-name	Контекст SNMPv3, используемый в процессе доступа. Применяется только в случае выбора протокола SNMPv3.
read-view	Представление этой группы будет использоваться GET-запросами. Диапазон - от 1 до 30 символов.
write-view	Представление этой группы будет использоваться SET-запросами. Диапазон - от 1 до 30 символов.
notify-view	Представление этой группы будет использоваться во время отправки trap. Диапазон - от 1 до 30 символов.

no snmp-server group

Команда удаляет указанную группу.

Формат no snmp-server group *group-name* {v1|v2c| 3 {noauth|auth|priv}} [context context-name]

Режим Global Config

snmp-server host

Данная команда настраивает отправку trap на определенный хост.

По умолчанию Хосты по умолчанию не настроены.

Формат snmp-server host *host-addr* {informs [timeout *seconds*] [retries *retries*]|traps version {1 | 2c }} community-string [udp-port *port*] [filter *filter-name*]

Режим Global Config

Параметр	Описание
host-addr	Адреса IPv4 и IPv6 хоста, для отправки trap или inform сообщений.
traps	Отправка SNMP-trap на хост. Этот параметр выбран по умолчанию.

Параметр	Описание
version 1	Отправляет SNMPv1 trap. Эта опция недоступна, если выбраны informs.
version 2	Отправляет SNMPv2c trap. Эта опция недоступна, если выбраны informs. Этот параметр выбран по умолчанию.
informs	Отправка SNMPv2 informs на хост.
seconds	Количество секунд ожидания подтверждения перед повторной отправкой Inform. Значение по умолчанию - 15. Диапазон - от 1 до 300 секунд.
retries	Количество повторных попыток отправки Inform. Значение по умолчанию - 3. Диапазон - от 0 до 255 попыток.
communitystring	Строка сообщества, отправленная в качестве части trap. Диапазон - от 1 до 20 символов.
port	Порт, принимающий SNMP trap. Порт по умолчанию - 162.
filter-name	Имя фильтра для ассоциации с этим хостом. Фильтры могут использоваться для выбора trap, посылаемых на хост. Диапазон - от 1 до 30 символов.

`no snmp-server host`

Данная команда удаляет указанную запись хоста.

Формат no snmp-server host *host-addr* [traps|informs]

Режим Global Config

`snmp-server user`

Данная команда создает пользователя SNMPv3 для доступа в систему.

По умолчанию Пользователь по умолчанию не создается.

Формат snmp-server user *username groupname* [remote *engineid-string*] [{auth-md5 *password* | auth-sha *password* | auth-md5-key *md5-key* | auth-sha-key *sha-key*} [priv-des *password* | priv-des-key *des-key*]

Режим Global Config

Параметр	Описание
username	Имя пользователя SNMPv3. Диапазон - от 1 до 30 символов.

Параметр	Описание
group-name	Название группы, к которой принадлежит пользователь. Диапазон - от 1 до 30 символов.
engineid-string	Engine-id удаленного устройства, с которого подключается пользователь. Диапазон - от 5 до 32 символов.
password	Пользовательский пароль используемый для аутентификации или шифрования. Диапазон - от 1 до 32 символов.
md5-key	Сгенерированный заранее ключ аутентификации MD5. Длина составляет 32 символа.
sha-key	Сгенерированный заранее ключ аутентификации SHA. Длина составляет 48 символов.
des-key	Сгенерированный заранее ключ шифрования DES. Длина составляет 32 символа при выборе MD5 и 48 символов при выборе SHA.

no snmp-server user

Команда удаляет указанного пользователя SNMPv3.

Формат no snmp-server user *username*

Режим Global Config

snmp-server view

Эта команда создает или изменяет существующую запись представления, которая используется группами для определения того, к каким объектам может обращаться сообщество или пользователь.

По умолчанию Представления создаются по умолчанию для доступа к группам по умолчанию.

Формат snmp-server *viewname oid-tree* {included|excluded}

Режим Global Config

Параметр	Описание
viewname	Название для создаваемого представления. Диапазон - от 1 до 30 символов.
oid-tree	Поддрево OID для включения в представление или исключения из него. Поддрева могут быть заданы численно (1.3.6.2.4) либо ключевым словом (system). Звездочки могут использоваться для определения семей поддрев (1.3.*.4).

Параметр	Описание
included	Древо включено в представление.
excluded	Древо исключено из представления.

no snmp-server view

Команда удаляет указанное представление.

Формат no snmp-server view *viewname* [*oid-tree*]

Режим Global Config

snmp-server v3-host

Данная команда настраивает trap, которые должны быть отправлены на определенный хост.

По умолчанию Хосты по умолчанию не настроены.

Формат snmp-server v3-host *host-addr username* [traps | informs [timeout *seconds*] [retries retries]] [auth | noauth | priv] [udpport *port*] [filter *filtername*]

Режим Global Config

Параметр	Описание
host-addr	Адреса IPv4 и IPv6 хоста, для отправки trap или inform сообщений.
user-name	Пользователь, отправляющий trap или inform сообщение. Пользователь должен быть ассоциирован с группой, поддерживающий версию и метод доступа. Диапазон - от 1 до 30 символов.
traps	Отправить SNMP trap на хост. Это настройка по умолчанию.
informs	Отправить SNMP inform на хост.
seconds	Количество секунд ожидания подтверждения перед повторной отпрвкой informs сообщения. Значение по умолчанию - 15. Диапазон - от 1 до 300 секунд.
retries	Количество повторных попыток отправки informs сообщения. Значение по умолчанию - 3. Диапазон - от 0 до 255 попыток.
auth	Включает аутентификацию, но не шифрование.
noauth	Без аутентификации или шифрования. Это настройка по умолчанию.

Параметр	Описание
priv	Включает и аутентификацию, и шифрование.
port	Порт, принимающий SNMP trap. Порт по умолчанию - 162.
filter-name	Имя фильтра для ассоциации с этим хостом. Фильтры могут использоваться для выбора trap, посылаемых на хост. Диапазон - от 1 до 30 символов.

snmptrap source-interface

Используйте данную команду в режиме Global Configuration для конфигурации глобального интерфейса-источника для всех SNMP-коммуникаций между SNMP-клиентом и сервером.

Формат snmptrap source-interface {*unit/slot/port* | vlan *vlan-id*}

Режим Global Configuration

Параметр	Описание
unit/slot/port	Идентификатор, назначенный коммутатору.
vlan-id	Настраивает интерфейс VLAN для использования в качестве IP-адреса источника. Диапазон VLAN ID - от 1 до 4093.

no snmptrap source-interface

Используйте данную команду в режиме Global Configuration для удаления глобального интерфейса-источника для всех SNMP-коммуникаций между SNMP-клиентом и сервером.

Формат no snmptrap source-interface

Режим Global Configuration

show snmp

Эта команда отображает текущую конфигурацию SNMP.

Формат snmp

Режим Privileged EXEC

Термин		Значение
Community Table:	Community-String	Строка сообщества для записи. Используется протоколами SNMPv1 и SNMPv2 для доступа к коммутатору.

Термин		Значение
Community Table:	CommunityAccess	Тип доступа, которым располагает сообщество: Read only Read write
	View Name	Предствление, к которому имеет доступ сообщество.
	IP Address	Доступ к этому сообществу ограничен этим IP-адресом.
Community Group Table:	Community-String	Сообщество, настраиваемое этой схемой.
	Group Name	Группа, к которой приписано данное сообщество.
	IP Address	IP-адрес, которым это сообщество ограничено.
Host Table:	Target Address	Адрес хоста, на который будут отправлены trap.
	Type	Тип посылаемого сообщения: trap или inform.
	Community	Сообщество, на которое будут отправлены trap.
	Version	Версия SNMP для отправки trap.
Host Table:	UDP Port	UDP-порт, на который будут отправлены trap или информация.
	Filter name	Фильтр, ограничивающий trap для данного хоста.
	TO Sec	Количество секунд, после которого отправленные на этот хост сообщения inform будут считаться устаревшими.
	Retries	Количество повторных попыток отправки сообщений inform после таймаута.

show snmp engineID

Эта команда отображает текущую конфигурацию SNMP engineID.

Формат show snmp engineID

Режим Privileged EXEC

Параметр	Описание
Local SNMP EnginID	Текущая конфигурация SNMP engineID.

show snmp filters

Эта команда отображает настроенные фильтры, используемые при отправке trap.

Формат show switch filters [*filtername*]

Режим Privileged EXEC

Параметр	Описание
Name	Имя фильтра для данной записи.
OID Tree	Древо OID, которое данная запись будет включать или исключать.
Type	Указывает на то, включает эта запись древо OID или исключает.

show snmp group

Эта команда показывает настроенные группы.

Формат show snmp group [*groupname*]

Режим Privileged EXEC

Параметр	Описание
Name	Имя группы.
Security Model	Указывает на то, какой протокол может получить доступ к системе через эту группу.
Security Level	Указывает уровень безопасности, разрешенный для этой группы.
Read View	Представление, к которому эта группа обеспечивает доступ с правом чтения.
Write View	Представление, к которому эта группа обеспечивает доступ с правом записи.

Параметр	Описание
Notify View	Представление, к которому эта группа обеспечивает доступ для отправки trap.

show snmp-server

Эта команда отображает текущую пользовательскую конфигурацию SNMP-сервера.

Формат show snmp-server

Режим Privileged EXEC

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing)#show snmp-server
SNMP Server Port.....161
```

show snmp source-interface

Используйте эту команду в режиме Privileged EXEC для отображения деталей настроенных глобальных интерфейсов-источников (IP-адресов источников), используемых SNMP-клиентом.

Формат show snmp source-interface

Режим Privileged EXEC

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing)# show snmp source-interface
SNMP trap Client Source Interface.....(not configured)
```

show snmp user

Эта команда отображает пользователей SNMPv3, настроенных в настоящее время.

Формат show snmp user [*username*]

Режим Privileged EXEC

Термин	Значение
Name	Имя пользователя.
Group Name	Группа, которая определяет параметры доступа SNMPv3.
Auth Method	Алгоритм аутентификации, настроенный для данного пользователя.
Privilege Method	Алгоритм шифрования для данного пользователя.
Remote Engine ID	EngineID для пользователя, определяемый на клиентской машине.

show snmp views

Эта команда отображает представления, настроенные в настоящее время.

Формат show snmp views [*viewname*]

Режим Privileged EXEC

Параметр	Описание
Name	Имя представления для данной записи.
OID Tree	Древо OID, которое данная запись будет включать или исключать.
Type	Указывает на то, включает эта запись древо OID или исключает.

show trapflags

Данная команда отображает условия отправки trap. Настройте trap, которые коммутатор должен генерировать путем включения или отключения условий отправки trap. Если условие отправки trap активировано и обнаружено, SNMP-агент на коммутаторе посылает trap всем возможным получателям. Внесение изменений не требует перезагрузки коммутатора. «Холодные» и «теплые» стартовые trap генерируются всегда и не могут быть отменены.

Формат show trapflags

Режим Privileged EXEC

Термин	Значение
Authentication Flag	Можно включить или отключить. По умолчанию - включено. Указывает, будет ли отправлен trap ошибки аутентификации.
Link Up/Down Flag	Можно включить или отключить. По умолчанию - включено. Указывает, будет ли отправлен trap состояния линка.
Multiple Users Flag	Можно включить или отключить. По умолчанию - включено. Указывает, будет ли отправлен trap когда пользователь с тем же user ID, авторизуется на коммутаторе более одного раза в один и тот же момент (либо по Telnet, либо по последовательному порту).
Spanning Tree Flag	Можно включить или отключить. По умолчанию - включено. Указывает, отправляются ли spanning tree traps.

5.10. Команды RADIUS

В этом разделе описаны команды, используемые для настройки сервера RADIUS (Remote Authentication Dial-In User Service) для аутентификации и учета.

aaa server radius dynamic-author

Данная команда активирует функционал CoA и переводит в режим конфигурации локального сервера динамической авторизации (Dynamic Authorization).

По умолчанию None

Формат aaa server radius dynamic-author

Режим Global Config

ПРИМЕР:

```
(Routing) #configure
(Routing) (Config)#aaa server radius dynamic-author
(Routing) (Config- radius-da)#
```

no aaa server radius dynamic-author

Данная команда отключает функциональность CoA.

По умолчанию None

Формат no aaa server radius dynamic-author

Режим Global Config

ПРИМЕР:

```
(Routing) #configure
(Routing) (Config)#no aaa server radius dynamic-author
```

auth-type

Данная команда указывает тип авторизации, используемый устройством для клиентов RADIUS. Для успешной авторизации клиент должен удовлетворять атрибутам, указанным при конфигурации.

По умолчанию All

Формат auth-type { any | all | session-key }

Режим Dynamic Authorization

ПРИМЕР:

```
(Routing) (Config- radius-da)#auth-type all
```

no auth-type

Данная команда сбрасывает тип авторизации, используемый устройством для клиентов RADIUS.

По умолчанию None

Формат no auth-type

Режим Dynamic Authorization

ПРИМЕР:

```
(Routing) (Config- radius-da)#no auth-type
```

clear radius dynamic-author statistics

Данная команда обнуляет счётчики динамической авторизации.

По умолчанию None

Формат clear radius dynamic-author statistics

Режим Privileged EXEC

ПРИМЕР:

(Routing) #clear radius dynamic-author statistics

Are you sure you want to clear statistics? (y/n) y

Statistics cleared.

client

Эта команда используется для настройки IP-адреса или имени хоста клиента сервера AAA. Используйте необязательное ключевое слово serverkey и строковый аргумент для настройки ключа сервера на уровне клиента.

По умолчанию None

Формат client { *ip-address* | *hostname* } [server-key [0|7] *key-string*]

Режим Dynamic Authorization

ПРИМЕР:

(Routing) (Config- radius-da)#client 10.0.0.1 server-key 7 device1

no client

Эта команда удаляет настроенный клиент динамической авторизации и ключ, ассоциируемый на устройстве с этим клиентом.

По умолчанию None

Формат no client { *ip-address* | *hostname* }

Режим Dynamic Authorization

ПРИМЕР:

(Routing) (Config- radius-da)#no client 10.0.0.1

debug aaa coa

Данная команда отображает информацию отладчика динамического сервера авторизации.

По умолчанию None

Формат debug aaa coa

Режим Privileged EXEC

debug aaa pod

Данная команда отображает пакеты Disconnect Message.

По умолчанию None

Формат debug aaa pod

Режим Privileged EXEC

ignore server-key

Данная необязательная команда настраивает устройство таким образом, что оно игнорирует ключ сервера.

По умолчанию Отключено

Формат ignore server-key

Режим Dynamic Authorization

ПРИМЕР:

```
(Routing) (Config- radius-da)#ignore server-key
```

no ignore server-key

Данная необязательная команда настраивает устройство таким образом, что оно перестаёт игнорировать ключ сервера (возвращаясь на настройки по умолчанию).

По умолчанию Отключено

Формат no ignore server-key

Режим Dynamic Authorization

ПРИМЕР:

```
(Routing) (Config- radius-da)#no ignore server-key
```

ignore session-key

Данная необязательная команда настраивает устройство таким образом, что оно игнорирует ключ сессии.

По умолчанию Отключено

Формат ignore session-key

Режим Dynamic Authorization

ПРИМЕР:

```
(Routing) (Config- radius-da)#ignore session-key
```

no ignore session-key

Данная необязательная команда настраивает устройство таким образом, что оно перестаёт игнорировать ключ сессии (возвращаясь на настройки по умолчанию).

По умолчанию Отключено

Формат no ignore session-key

Режим Dynamic Authorization

ПРИМЕР:

```
(Routing) (Config- radius-da)#no ignore session-key
```

port

Используйте эту команду для указания UDP-порта, на котором устройство будет слушать RADIUS-запросы от клиентов динамической авторизации. Поддерживаемый диапазон портов: 1025 – 65535.

По умолчанию 3799

Формат port *port-number*

Режим Dynamic Authorization

ПРИМЕР:

```
(Routing) (Config- radius-da)#port 1700
```

no port

Используйте эту команду для сброса настроек UDP-порта для RADIUS-запросов на заводские настройки.

По умолчанию 3799

Формат no port

Режим Dynamic Authorization

ПРИМЕР:

```
(Routing) (Config- radius-da)#no port
```

radius accounting mode

Данная команда включает функцию учета RADIUS.

По умолчанию disabled

Формат radius accounting mode

Режим Global Config

no radius accounting mode

Данная команда сбрасывает функцию учета RADIUS на заводские значения (то есть, отключает ее).

Формат no radius accounting mode

Режим Global Config

radius server attribute 4

Данная команда настраивает клиент RADIUS для использования атрибута NAS-IP Address в RADIUS-запросах. Если определенный IP-адрес настроен при включенном атрибуте, RADIUS-клиент использует этот IP-адрес при отправке атрибута NAS-IP Address в RADIUS-коммуникации.

Формат radius server attribute 4 [*ipaddr*]

Режим Global Config

Термин	Значение
4	Атрибут NAS-IP Address для использования в запросах RADIUS.
ipaddr	IP-адрес сервера.

no radius server attribute 4

«No»-версия данной команды отключает глобальные параметры атрибута NAS-IP Address для клиентов RADIUS. Если этот параметр отключен, клиент RADIUS не отправляет атрибут NAS-IP-Address в RADIUS-запросах.

Формат no radius server attribute 4 [*ipaddr*]

Режим Global Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Switch) (Config) #radius server attribute 4  192.168.37.60
(Switch) (Config) #radius server attribute 4
```

radius server attribute 26 dhcp

Данная команда настраивает клиент RADIUS для использования атрибута Vendor-Specific в RADIUS-запросах. Если настроены параметры протокола dhcp, RADIUS-клиент использует эти параметры при отправке атрибута в RADIUS-коммуникации.

Формат radius server attribute 26 dhcp [*class-ident* | *hostname* | *client-ident*]

Режим Global Config

Термин	Значение
26	Атрибут Vendor-Specific для использования в запросах RADIUS.
class-ident	Идентификатор поставщика
hostname	Имя клиента
client-ident	Идентификатор клиента

no radius server attribute 26 dhcp [class-ident | hostname | client-ident]

«No»-версия данной команды отключает настроенные параметры атрибута Vendor-Specific для клиентов RADIUS. Если эти параметр отключены, клиент RADIUS не отправляет атрибут Vendor-Specific с указанными параметрами в RADIUS-запросах.

Формат no radius server attribute 26 dhcp [*class-ident* | *hostname* | *client-ident*]

Режим Global Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Switch) (Config) # radius server attribute 26 dhcp class-ident
(Switch) (Config) # radius server attribute 26 dhcp hostname
(Switch) (Config) # radius server attribute 26 dhcp client-ident
```

radius server attribute 26 lldp

Данная команда настраивает клиент RADIUS для использования атрибута Vendor-Specific в RADIUS-запросах. Если настроены параметры протокола lldp, RADIUS-клиент использует эти параметры при отправке атрибута в RADIUS-коммуникации.

Формат radius server attribute 26 lldp [*port-desc* | *sys-name* | *sys-desr*]

Режим Global Config

Термин	Значение
26	Атрибут Vendor-Specific для использования в запросах RADIUS.
port-descr	Описание порта
sys-name	Имя устройства
sys-descr	Описание устройства

no radius server attribute 26 lldp [*port-desc* / *sys-name* / *sys-desr*]

«No»-версия данной команды отключает настроенные параметры атрибута Vendor-Specific для клиентов RADIUS. Если эти параметры отключены, клиент RADIUS не отправляет атрибут Vendor-Specific с указанными параметрами в RADIUS-запросах.

Формат no radius server attribute 26 lldp [*port-desc* | *sys-name* | *sys-desr*]

Режим Global Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Switch) (Config) # radius server attribute 26 lldp port-descr
(Switch) (Config) # radius server attribute 26 lldp sys-name
(Switch) (Config) # radius server attribute 26 lldp sys-descr
```

radius server host

Данная команда позволяет настроить IP-адрес или DNS-имя для взаимодействия с RADIUS-сервером выбранного типа. При настройке IP-адреса или DNS-имени для серверов идентификации или учета можно также настроить номер порта и имя сервера. Если сервера идентификации и учета сконфигурированы без имени, то команда использует имена Default_RADIUS_Auth_Server и Default_RADIUS_Acct_Server соответственно. Имена серверов аутентификации могут повторяться, имена серверов учёта должны быть уникальными. Клиент RADIUS позволяет настраивать до 32 серверов аутентификации и учета.

Если вы используете параметр *auth*, команда настраивает IP-адрес или имя хоста для подключения к серверу аутентификации RADIUS. Вы можете настроить до 3 серверов на каждого клиента RADIUS. Если достигнуто максимальное количество серверов, команда не выполняется до тех пор, пока вы не удалите один из серверов при помощи «No»-версии команды. Если вы используете необязательный параметр *port*, команда настраивает номер порта UDP для использования при подключении к настроенному серверу RADIUS. Диапазон портов: 1 – 65535, порт по умолчанию: 1812.

ПРИМЕЧАНИЕ: Для перенастройки сервера аутентификации RADIUS на использование порта UDP по умолчанию, настройте параметр *port* на 1812.

Если вы используете параметр **acct**, команда настраивает IP-адрес или имя хоста для подключения к серверу учета RADIUS. Вы можете настроить только один сервер учета. Если сервер учета уже настроен, используйте «No»-версию команды, чтобы удалить текущую конфигурацию. Указанный IP-адрес или имя хоста должны совпадать с предварительно настроенным сервером учета. Если вы используете необязательный параметр **port**, команда настраивает номер порта UDP для использования при подключении к настроенному серверу учета RADIUS. Если **port** уже настроен для сервера учета, новое значение **port** заменит предыдущее. Значение **port** должно быть в пределах диапазона 0 – 65535, порт 1813 выбран по умолчанию.

ПРИМЕЧАНИЕ: Для перенастройки сервера учета RADIUS на использование порта UDP по умолчанию, установите параметр **port** на 1813.

Формат radius server host {auth | acct} {*ipaddr*|*dnsname*} [name *servername*] [port *0-65535*]

Режим Global Config

Поле	Описание
ipaddr	IP-адрес сервера.
dnsname	DNS-имя сервера.
0-65535	Номер порта, используемый для соединения с указанным сервером RADIUS.
servername	Имя, используемое для идентификации сервера.

no radius server host

«No»-версия данной команды удаляет настроенную запись сервера из списка настроенных серверов RADIUS. Если сервер аутентификации RADIUS удален, но существует другой сервер с тем же именем, RADIUS-клиенты будут использовать его. Если используется ключевое слово **'auth'**, предыдущий сервер аутентификации RADIUS будет удален из конфигурации. Ключевое слово **'acct'** похожим образом удаляет сервер учета RADIUS. Параметр **ipaddr|dnsname** должен совпадать с IP-адресом или именем DNS ранее настроенного сервера RADIUS (учета либо аутентификации).

Формат no radius server host {auth | acct} {*ipaddr*|*dnsname*}

Режим Global Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Switch) (Config) #radius server host acct 192.168.37.60
```

(Switch) (Config) #radius server host acct 192.168.37.60 port 1813

(Switch) (Config) #radius server host auth 192.168.37.60 name Network1_RS port 1813

(Switch) (Config) #radius server host acct 192.168.37.60 name Network2_RS

(Switch) (Config) #no radius server host acct 192.168.37.60

radius server host test

Данная команда активирует функцию проверки доступности RADIUS-сервера с помощью тестового пользователя.

ПРИМЕЧАНИЕ: Указываемый тестовый пользователь должен содержаться в локальной базе пользователей коммутатора.

Формат radius server host test *username*

Режим Global Config

Поле	Описание
username	Имя тестового пользователя

no radius server host test

Данная команда отключает функцию проверки доступности RADIUS-сервера с помощью тестового пользователя

Формат no radius server host test *username*

Режим Global Config

radius server deadtime

Данная команда указывает временной промежуток, в течении которого коммутатор не обращается на RADIUS-сервер, если текущий статус RADIUS-сервера отмечен как DEAD.

По умолчанию 0

Формат radius server deadtime *time*

Режим Global Config

Поле	Описание
time	Время в минутах

no radius server deadtime

Данная команда возвращает значение deadtime к настройкам по-умолчанию.

Формат no radius server deadtime *time*

Режим Global Config

radius server key

Данная команда настраивает ключ, используемый при коммуникации клиента и определенного сервера RADIUS. В зависимости от того, какое ключевое слово используется: 'auth' или 'acct' - общий секретный ключ настраивается для RADIUS-сервера аутентификации либо учета. Указанный IP-адрес или имя хоста должны совпадать с предварительно настроенным сервером. При выполнении команды запрашивается секретный ключ.

Текстовая конфигурация поддерживает секретные ключи сервера RADIUS как в зашифрованном, так и в не зашифрованном форматах. При сохранении конфигурации данные секретные ключи хранятся только в зашифрованном виде. Если вы хотите ввести ключ в зашифрованном формате, введите ключ вместе с ключевым словом «encrypted». При выполнении команды **show running-config** эти секретные ключи отображаются в зашифрованном формате. Вы не можете показать эти ключи в формате обычного текста.

ПРИМЕЧАНИЕ: Секретный ключ должен состоять из не более чем 16 цифр и/или букв.

Формат radius server key {auth | acct} {*ipaddr*|*dnsname*} *encrypted password*

Режим Global Config

Поле	Описание
ipaddr	IP-адрес сервера.
dnsname	DNS-имя сервера.
password	Пароль в зашифрованном формате.

ПРИМЕР: Ниже приведен пример команды.

radius server key acct 10.240.4.10 encrypted ***encrypt-string***

radius server msgauth

Данная команда активирует функцию проверки подлинности сообщения, используемого для определенного RADIUS-сервера аутентификации.

Формат radius server msgauth *ipaddr*|*dnsname*

Режим Global Config

Поле	Описание
ip addr	IP-адрес сервера.
dnsname	DNS-имя сервера.

no radius server msgauth

Данная команда отключает функцию проверки подлинности сообщения, используемого для определенного RADIUS-сервера аутентификации.

Формат no radius server msgauth *ipaddr*|*dnsname*

Режим Global Config

radius server primary

Данная команда позволяет выбрать первичный сервер из группы настроенных серверов с одним и тем же именем. Можно настроить несколько первичных серверов, по одному для каждой такой группы. Когда клиент RADIUS должен выполнять операции с сервером аутентификации RADIUS, имеющим указанное имя, клиент использует первичный сервер, имеющий указанное имя по умолчанию. Если взаимодействие между клиентом и первичным сервером по каким-либо причинам невозможно, клиент использует резервные серверы, на которых настроено то же имя. Эти резервные серверы считются вспомогательными.

Формат radius server primary {*ipaddr*|*dnsname*}

Режим Global Config

Поле	Описание
ip addr	IP-адрес сервера аутентификации RADIUS.
dnsname	DNS-имя сервера.

radius server retransmit

Эта команда настраивает глобальный параметр для клиента RADIUS, задающий количество передач сообщений, которые должны быть сделаны, прежде чем будет произведена попытка связаться с вспомогательным сервером аутентификации RADIUS. Если максимальное количество попыток для сервера учета RADIUS будет исчерпано и ответ не будет получен, клиент не связывается с каким-либо другим сервером.

По умолчанию 4

Формат radius server retransmit *retries*

Режим Global Config

Поле	Описание
retries	Максимальное количество попыток передачи в диапазоне от 1 до 15.

no radius server retransmit

«No»-версия данной команды сбрасывает значение параметра значения по умолчанию.

Формат no radius server retransmit

Режим Global Config

radius source-interface

Используйте эту команду, чтобы указать физический или логический интерфейс для использования в качестве интерфейса источника клиента RADIUS (IP-адрес источника). Если адрес исходного интерфейса настроен, он используется для всех RADIUS-коммуникаций между сервером и клиентом. Выбранный IP-адрес интерфейса-источника используется для заполнения IP-заголовка пакетов протокола

управления RADIUS. Это позволяет устройствам безопасности (межсетевым экранам) определять исходные пакеты, исходящие от конкретного коммутатора.

Если интерфейс-источник не указан, первичный IP-адрес исходящего интерфейса используется в качестве исходного адреса. Если сконфигурированный интерфейс не работает, клиент RADIUS возвращается к его поведению по умолчанию.

Формат radius source-interface {*unit/slot/port* | loopback *loopback-id* | vlan *vlan-id*}

Режим Global Config

Параметр	Описание
unit/slot/port	Идентификатор, назначенный коммутатору.
loopback-id	Настройка loopback-интерфейса. Диапазон loopback ID - от 0 до 7.
vlan-id	Настраивает интерфейс VLAN для использования с IP-адресом источника. Диапазон VLAN ID - от 1 до 4093.

no radius source-interface

Данная команда используется для сброса интерфейса-источника RADIUS на настройки по умолчанию.

Формат no radius source-interface

Режим Global Config

radius server timeout

Эта команда настраивает глобальный параметр для клиента RADIUS, указывающий значение таймаута (в секундах), после которого запрос должен быть повторно передан на сервер RADIUS, если ответ не получен. Значение таймаута - целое число в диапазоне от 1 до 30.

По умолчанию 5

Формат radius server timeout *seconds*

Режим Global Config

Поле	Описание
retries	Максимальное количество попыток передачи в диапазоне от 1 до 30.

no radius server timeout

«No»-версия данной команды сбрасывает таймаут на значения по умолчанию.

Формат no radius server timeout

Режим Global Config

server-key

Используйте эту команду для настройки общего общего секретного ключа, который используется для всех клиентов динамической авторизации, для которых не настроен индивидуальный секретный ключ.

По умолчанию None

Формат server-key [7] *key-string*

Режим Dynamic Authorization

Термин	Значение
0	Необходимо ввести незашифрованный ключ
7	Необходимо ввести зашифрованный ключ
string	Общая секретная строка. Максимальная длина составляет 128 символов для незашифрованного ключа и 256 символов - для зашифрованного. Переопределяет глобальные настройки только для этого клиента. Для использования спецсимволов или пробелов заключите их в кавычки.

ПРИМЕР:

```
(Routing) (Config-radius-da)# server-key encrypted mydevice
```

no server-key

Данная команда используется для удаления конфигурации глобального общего секретного ключа.

По умолчанию None

Формат no server-key

Режим Dynamic Authorization

ПРИМЕР:

```
(Routing) (Config-radius-da)#no server-key
```

show radius

Данная команда отображает значения настроенных глобальных параметров для клиента RADIUS.

Формат show radius

Режим Privileged EXEC

Термин	Значение
Number of Configured Authentication Servers	Количество настроенных серверов аутентификации RADIUS.

Термин	Значение
Number of Configured Accounting Servers	Количество настроенных серверов учета RADIUS.
Number of Named Authentication Server Groups	Количество групп RADIUS-серверов аутентификации, имеющих имя.
Number of Named Accounting Server Groups	Количество групп RADIUS-серверов учета, имеющих имя.
Deadtime	Время неактивности (в минутах) серверов аутентификации RADIUS.
Number of Retransmits	Настроенное значение максимального количества повторных передач пакета запроса.
Time Duration	Настроенное значение таймаута (в секундах) для повторной передачи запроса.
RADIUS Accounting Mode	Глобальный параметр, указывающий, включен ли режим учета для всех серверов.
RADIUS Attribute 4 Mode	Глобальный параметр, указывающий, разрешен ли атрибут NAS-IP-Address для использования в RADIUS-запросах.
RADIUS Attribute 4 Value	Глобальный параметр, который определяет IP-адрес, используемый в атрибуте NAS-IP-Address для использования в RADIUS-запросах.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Switch) #show radius
Number of Configured Authentication Servers.....32
Number of Configured Accounting Servers .....32
Number of Named Authentication Server Groups.....15
Number of Named Accounting Server Groups.....3
Number of Retransmits .....4
Deadtime .....1
Time Duration.....10
RADIUS Accounting Mode .....Disable
```

RADIUS Attribute 4 Mode.....Enable

RADIUS Attribute 4 Value 192.168.37.60

Radius test user.....test_user

show radius servers

Эта команда отображает сводную информацию и подробные сведения о серверах аутентификации RADIUS, настроенных для RADIUS-клиента.

Формат show radius servers [{*ipaddr*|*dnsname* | name [servername]}]

Режим Privileged EXEC

Поле	Описание
ipaddr	IP-адрес сервера аутентификации.
dnsname	DNS-имя сервера аутентификации.
servername	Имя, используемое для идентификации сервера.
Current	Символ * перед адресом сервера указывает, что в данный момент сервер является активным.
Поле	Описание
Host Address	IP-адрес хоста.
Server Name	Имя сервера аутентификации.
Порты	Порт, используемый для связи с сервером аутентификации.
Type	Указывает, будет ли данный сервер является первичным или вспомогательным.
Deadtime	Время неактивности (в минутах) серверов аутентификации RADIUS.
ServerIsDead	Логическое значение "Да" или "Нет", указывающее, отмечен ли статус данного сервера как "Dead"
Resurrection in	Время (в секундах), оставшееся до изменения статуса данного сервера на "Alive"
Current Host Address	IP-адрес сервера аутентификации, активного в настоящий момент.
Secret Configured	Логическое значение "Да" или "Нет", указывающее, сконфигурирован ли данный сервер с секретным паролем.

Поле	Описание
Number of Retransmits	Настроенное значение максимального количества повторных передач пакета запроса.
Message Authenticator	Глобальный параметр, указывающий, активирован ли атрибут проверки подлинности сообщения.
Time Duration	Настроенное значение таймаута (в секундах) для повторной передачи запроса.
RADIUS Accounting Mode	Глобальный параметр, указывающий, включен ли режим учета для всех серверов.
RADIUS Attribute 4 Mode	Глобальный параметр, указывающий, включен ли атрибут NAS-IP-Address для использования в запросах RADIUS.
RADIUS Attribute 4 Value	Глобальный параметр, который определяет IP-адрес, используемый в атрибуте NAS-IP-Address для использования в запросах RADIUS.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Switch) #show radius servers

*   Host Address       Server Name               Port       Type        Status
-   ------------------ ------------------------- ---------  ----------- ---------
*   192.168.37.200     Network1_RADIUS_Server    1812       Primary     Alive
*   192.168.37.201     Network2_RADIUS_Server    1812       Secondary   Alive
*   192.168.37.202     Network3_RADIUS_Server    1812       Secondary   Alive
*   192.168.37.203     Network4_RADIUS_Server    1812       Secondary   Alive
* currently selected server

(Switch) #show radius servers name

   Current Host Address        Server Name                  Type
 --------------------------- --------------------------- --------------------------
   192.168.37.200              Network1_RADIUS_Server       Secondary
   192.168.37.201              Network2_RADIUS_Server       Primary
   192.168.37.202              Network3_RADIUS_Server       Secondary
   192.168.37.203              Network4_RADIUS_Server       Primary
```

```
(Switch) #show radius servers name Default_RADIUS_Server
RADIUS Server Name ..... Default-RADIUS-Server
Current Server IP Address..... 192.168.37.60
Number of Retransmits ..... 3
Timeout Duration ..... 5
RADIUS Accounting Mode ..... Enable
RADIUS Attribute 4 Mode..... Enable
RADIUS Attribute 4 Value ..... 192.168.37.60
Port..... 1812
Type ..... Secondary
Deadtime ..... 0
ServerIsDead ..... No
Resurrection in..... 0 sec
Secret Configured ..... Yes
Message Authenticator ..... Enable
Number of CoA Requests Received..... 0
Number of CoA ACK Responses Sent..... 0
Number of CoA NAK Responses Sent ..... 0
Number of CoA Requests Ignored..... 0
Number of CoA Missing/Unsupported Attribute R..... 0
Number of CoA Session Context Not Found Reque ..... 0
Number of CoA Invalid Attribute Value Request ..... 0
Number of Administratively Prohibited Request..... 0

(Switch) #show radius servers secure-network.local
RADIUS Server DNS Address..... secure-network.local
RADIUS Server IP Address ..... 192.168.37.61
RADIUS Server Name ..... Default-RADIUS-Server
Number of Retransmits ..... 3
Timeout Duration ..... 5
RADIUS Accounting Mode ..... Enable
RADIUS Attribute 4 Mode..... Enable
RADIUS Attribute 4 Value ..... 192.168.37.61
Port..... 1812
Type ..... Secondary
Deadtime ..... 0
ServerIsDead ..... No
```

Resurrection in..... 0 sec
Secret Configured ..... No
Message Authenticator ..... Enable
Number of CoA Requests Received..... 0
Number of CoA ACK Responses Sent..... 0
Number of CoA NAK Responses Sent 0
Number of CoA Requests Ignored..... 0
Number of CoA Missing/Unsupported Attribute R..... 0
Number of CoA Session Context Not Found Reque 0
Number of CoA Invalid Attribute Value Request 0
Number of Administratively Prohibited Request..... 0

(Switch) #show radius servers 192.168.37.60
RADIUS Server IP Address 192.168.37.60
RADIUS Server Name..... Default-RADIUS-Server
Number of Retransmits..... 3
Timeout Duration 5
RADIUS Accounting Mode ..... Enable
RADIUS Attribute 4 Mode..... Enable
RADIUS Attribute 4 Value 192.168.37.60
Port..... 1812
Type..... Secondary
Deadtime..... 0
ServerIsDead ..... No
Resurrection in..... 0 sec
Secret Configured ..... Yes
Message Authenticator ..... Enable

show radius accounting

Эта команда отображает сводную информацию о настроенных серверах учета RADIUS.

Формат show radius accounting name [*servername*]

Режим Privileged EXEC

Поле	Описание
servername	Имя, используемое для идентификации сервера.

Поле	Описание
RADIUS Accounting Mode	Глобальный параметр, указывающий, включен ли режим учета для всех серверов.

Если вы не укажете какие-либо параметры, отобразится только режим учета и данные сервера учета RADIUS.

Термин	Значение
Host Address	IP-адрес хоста.
Server Name	Имя сервера учета.
Порты	Порт, используемый для связи с сервером учета.
Secret Configured	Логическое значение "Да" или "Нет", указывающее, сконфигурирован ли данный сервер с секретным паролем.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Switch) #show radius accounting name

Host Address          Server Name                Port          Secret Configured
-------------------------------------------------------------------------------
192.168.37.200        Network1_RADIUS_Server     1813          Yes
192.168.37.201        Network2_RADIUS_Server     1813          No
192.168.37.202        Network3_RADIUS_Server     1813          Yes
192.168.37.203        Network4_RADIUS_Server     1813          No

(Switch) #show radius accounting name Default_RADIUS_Server
Server Name ..... Default_RADIUS_Server
Host Address..... 192.168.37.200
RADIUS Accounting Mode ..... Disable
Port..... 1813 Secret
Configured..... Yes
```

show radius accounting statistics

Эта команда отображает статистику серверов учета RADIUS.

Формат show radius accounting statistics {*ipaddr*|*dnsname* | name *servername*}

Режим Privileged EXEC

Термин	Значение
ipaddr	IP-адрес сервера.
dnsname	DNS-имя сервера.
servername	Имя, используемое для идентификации сервера.
RADIUS Accounting Server Name	Имя сервера учета.
Server Host Address	IP-адрес хоста.
Round Trip Time	Интервал времени, в сотых долях секунды, между последним Accounting-Response и Accounting-Request, который соответствовал ему с данного сервера учета RADIUS.
Requests	Количество пакетов Accounting-Request RADIUS, отправленных на этот сервер. Это число не учитывает повторную передачу пакетов.
Retransmission	Количество пакетов Accounting-Request RADIUS, повторно отправленных на этот сервер.
Responses	Количество RADIUS-пакетов, полученных на порт учета с этого сервера.
Malformed Responses	Количество ошибочных пакетов RADIUS Accounting-Response, полученных с этого сервера. Ошибочные пакеты включают в себя пакеты некорректной длины. Некорректные аутентификаторы или атрибуты подписи, а также неизвестные типы не учитываются.
Bad Authenticators	Количество пакетов RADIUS Accounting-Response, содержащих некорректные аутентификаторы и полученных с этого сервера.
Pending Requests	Количество пакетов RADIUS Accounting-Request, отправленных на этот сервер, время ожидания которых не истекло, или которые не получили ответ.
Timeouts	Количество тайм-аутов учета для этого сервера.
Unknown Types	Количество RADIUS-пакетов неизвестных типов, которые были получены с этого сервера на порт учета.

Термин	Значение
Packets Dropped	Количество RADIUS-пакетов, полученных с данного сервера на порт учета, которые были отклонены по какой либо иной причине.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Switch) #show radius accounting statistics 192.168.37.200
RADIUS Accounting Server Name..... Default_RADIUS_Server
Host Address..... 192.168.37.200
Round Trip Time ..... 0.00
Requests ..... 0
Retransmissions..... 0
Responses..... 0
Malformed Responses ..... 0
Bad Authenticators..... 0
Pending Requests ..... 0
Timeouts..... 0
Unknown Types ..... 0
Packets Dropped ..... 0

(Switch) #show radius accounting statistics name Default_RADIUS_Server
RADIUS Accounting Server Name..... Default_RADIUS_Server
Host Address..... 192.168.37.200
Round Trip Time ..... 0.00
Requests ..... 0
Retransmissions..... 0
Responses..... 0
Malformed Responses ..... 0
Bad Authenticators..... 0
Pending Requests ..... 0
Timeouts..... 0
Unknown Types ..... 0
Packets Dropped ..... 0
```

show radius source-interface

Используйте эту команду в режиме Privileged EXEC для отображения информации о настроенном клиентском интерфейсе источника RADIUS (IP-адрес источника).

Формат show radius source-interface

Режим Privileged EXEC

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing)# show radius source-interface
RADIUS Client Source Interface..... (not configured)
```

show radius statistics

Эта команда отображает статистику настроенных серверов аутентификации RADIUS.

Формат show radius statistics {*ipaddr*|*dnsname* | name *servername*}

Режим Privileged EXEC

Термин	Значение
ipaddr	IP-адрес сервера.
dnsname	DNS-имя сервера.
servername	Имя, используемое для идентификации сервера.
RADIUS Server Name	Имя сервера аутентификации.
Server Host Address	IP-адрес хоста.
Access Requests	Количество пакетов Access-Request RADIUS, отправленных на этот сервер. Это число не учитывает повторную передачу пакетов.
Access Retransmissions	Количество пакетов Access-Request RADIUS, повторно отправленных на этот сервер аутентификации RADIUS.
Access Accepts	Количество пакетов RADIUS Access-Accept (включая как действительные, так и недействительные пакеты), полученных с этого сервера.
Access Rejects	Количество пакетов RADIUS Access-Reject (включая как действительные, так и недействительные пакеты), полученных с этого сервера.
Access Challenges	Количество пакетов RADIUS Access-Challenge (включая как действительные, так и недействительные пакеты), полученных с этого сервера.

Термин	Значение
Malformed Access Responses	Количество ошибочных пакетов RADIUS Access-Response, полученных с этого сервера. Ошибочные пакеты включают в себя пакеты некорректной длины. Некорректные аутентификаторы или атрибуты подписи, а также неизвестные типы не учитываются.
Bad Authenticators	Количество пакетов RADIUS Access-Response, содержащих некорректные аутентификаторы или сигнатуры, полученных с этого сервера.
Pending Requests	Количество пакетов RADIUS Access-Request, отправленных на этот сервер, время ожидания которых не истекло, или которые не получили ответ.
Timeouts	Количество тайм-аутов аутентификации для этого сервера.
Unknown Types	Количество-пакетов неизвестных типов, которые были получены с этого сервера на порт аутентификации.
Packets Dropped	Количество RADIUS-пакетов, полученных с данного сервера на порт аутентификации, которые были отклонены по какой либо иной причине.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Switch) #show radius statistics 192.168.37.200
RADIUS Server Name ..... Default_RADIUS_Server
Server Host Address ..... 192.168.37.200
Access Requests ..... 0.00
Access Retransmissions..... 0
Access Accepts ..... 0
Access Rejects ..... 0
Access Challenges..... 0
Malformed Access Responses ..... 0
Bad Authenticators..... 0
Pending Requests ..... 0
Timeouts..... 0
Unknown Types ..... 0
Packets Dropped ..... 0

(Switch) #show radius statistics name Default_RADIUS_Server
RADIUS Server Name ..... Default_RADIUS_Server
```

Server Host Address 192.168.37.200
Access Requests 0.00
Access Retransmissions..... 0
Access Accepts..... 0
Access Rejects..... 0
Access Challenges..... 0
Malformed Access Responses 0
Bad Authenticators..... 0
Pending Requests 0
Timeouts..... 0
Unknown Types 0
Packets Dropped 0

5.11. Команды TACACS+

TACACS + обеспечивает контроль доступа для сетевых устройств через один или несколько централизованных серверов. Подобно RADIUS, этот протокол упрощает аутентификацию, используя единую базу данных, которая может использоваться многими клиентами в большой сети. TACACS + основан на протоколе TACACS (описанном в RFC1492), но дополнительно предусматривает отдельные службы аутентификации, авторизации и учета. Исходным протоколом был UDP, основанный на сообщениях, переданных по сети в виде открытого текста. TACACS + использует TCP для обеспечения надежной доставки и общий ключ, настроенный на клиенте и демоне сервера для шифрования всех сообщений.

tacacs-server host

Используйте данную команду в режиме Global Configuration для настрйоки сервера TACACS+. Команда активирует режим конфигурации TACACS+. Параметр **ip-address|hostname** - это IP-адрес или имя хоста сервера TACACS+. Для указания нескольких хостов используйте команду **tacacs-server host** несколько раз.

Формат tacacs-server host *ip-address|hostname*

Режим Global Config

no tacacs-server host

Данная команда удаляет указанное имя хоста или IP-адрес. Параметр *ip-address|hostname* - это IP-адрес или имя хоста сервера TACACS+.

Формат no tacacs-server host *ip-address|hostname*

Режим Global Config

tacacs-server key

Данная команда настраивает ключ аутентификации и шифрования для всех коммуникаций TACACS+ между коммутатором и демоном TACACS+. Параметр **key-string** имеет диапазон 0 – 128 символов и задает ключ аутентификации и шифрования для всех

коммуникаций TACACS+ между коммутатором и сервером TACACS+. Ключ должен соответствовать тому, что используется в демоне TACACS+.

Текстовая конфигурация поддерживает секретные ключи сервера TACACS как в зашифрованном, так и в не зашифрованном форматах. При сохранении конфигурации данные секретные ключи хранятся только в зашифрованном виде. Если вы хотите ввести ключ в зашифрованном формате, введите ключ вместе с ключевым словом «**encrypted**». При выполнении команды **show running-config** эти секретные ключи отображаются в зашифрованном формате. Вы не можете показать эти ключи в формате обычного текста.

Формат tacacs-server key [*key-string* | encrypted *key-string*]

Режим Global Config

no tacacs-server key

Данная команда деактивирует ключ аутентификации и шифрования для всех коммуникаций TACACS+ между коммутатором и демоном TACACS+. Параметр *key-string* имеет диапазон от 0 до 128 символов. Ключ должен соответствовать тому, что используется в демоне TACACS+.

Формат no tacacs-server key *key-string*

Режим Global Config

tacacs-server keystring

Данная команда настраивает глобальный ключ аутентификации и шифрования для всех коммуникаций TACACS+ между сервером и клиентом TACACS+.

Формат tacacs-server keystring

Режим Global Config

ПРИМЕР: Ниже приведен пример команды.

```
(Switching)(Config)#tacacs-server keystring
Enter tacacs key:********
Re-enter tacacs key:********
```

tacacs-server source-interface

Используйте данную команду в режиме Global Configuration для настройки интерфейса-источника (IP-адреса источника) для конфигурации сервера TACACS+. Выбранный IP-адрес интерфейса-источника используется для заполнения IP-заголовка пакетов протокола управления. Это позволяет устройствам безопасности (межсетевым экранам) определять пакеты, исходящие от конкретного коммутатора.

Если интерфейс-источник не указан, первичный IP-адрес исходящего интерфейса используется в качестве исходного адреса.

Формат tacacs-server source-interface {*unit/slot/port*|loopback *loopback-id*|vlan *vlan-id*}

Режим Global Config

Параметр	Описание
unit/slot/port	Идентификатор, присвоенный коммутатору, в формате unit/slot/port.
loopback-id	Loopback-интерфейс. Диапазон loopback ID - от 0 до 7.
vlan-id	Настраивает интерфейс VLAN для использования с IP-адресом источника. Диапазон VLAN ID - от 1 до 4093.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Config)#tacacs-server source-interface loopback 0
(Config)#tacacs-server source-interface 1/0/1
(Config)#no tacacs-server source-interface
```

no tacacs-server source-interface

Используйте данную команду в режиме Global Configuration для удаления глобального интерфейса-источника для всех коммуникаций TACACS+ между клиентом и сервером.

Формат no tacacs-server source-interface

Режим Global Config

tacacs-server timeout

Используйте данную команду для настройки значения таймаута для коммуникации в пределах серверов TACACS+. Параметр **timeout** имеет диапазон 1 – 30. Измеряется в секундах. Если не задать значение тайм-аута, команда устанавливает глобальные тайм-аут по умолчанию. Сервера TACACS+, не использующие глобальные таймауты, сохранят собственную конфигурацию таймаутов.

По умолчанию 5

Формат tacacs-server timeout *timeout*

Режим Global Config

no tacacs-server timeout

Используйте данную команду для значения таймаута для коммуникации в пределах серверов TACACS на настройки по умолчанию.

Формат no tacacs-server timeout

Режим Global Config

key

Используйте команду **key** в режиме TACACS Configuration, чтобы указать ключ аутентификации и шифрования для всех сообщений TACACS между устройством и сервером. Ключ должен соответствовать тому, что используется в демоне TACACS. Параметр **key-string** задает имя ключа. Для пустого имени используйте “ ”. (Диапазон: 0 – 128 символов).

Текстовая конфигурация поддерживает секретные ключи сервера TACACS как в зашифрованном, так и в не зашифрованном форматах. При сохранении конфигурации данные секретные ключи хранятся только в зашифрованном виде. Если вы хотите ввести ключ в зашифрованном формате, введите ключ вместе с ключевым словом «encrypted». При выполнении команды **show running-config** эти секретные ключи отображаются в зашифрованном формате. Вы не можете показать эти ключи в формате обычного текста.

Формат key [*key-string* | encrypted *key-string*]

Режим TACACS Config

keystring

Используйте команду **keystring** в режиме TACACS Server Configuration, чтобы установить серверный ключ аутентификации и шифрования TACACS+ для всех сообщений TACACS между клиентом и сервером.

Формат keystring

Режим TACACS Server Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Switching)(Config)#tacacs-server host 1.1.1.1
(Switching)(Tacacs)#keystring
Enter tacacs key:********
Re-enter tacacs key:********
```

port

Используйте данную команду в режиме TACACS Configuration, чтобы указать номер порта сервера. Значение *portnumber* принадлежит диапазону 0 - 65535.

По умолчанию 49

Формат port port-number

Mode TACACS Config

priority (TACACS Config)

Используйте команду **priority** в режиме TACACS Configuration, чтобы указать порядок, в котором должны использоваться сервера. 0 (ноль) - высший приоритет. Параметр **priority** указывает приоритет серверов. Высший приоритет - 0, диапазон: 0 – 65535.

По умолчанию 0

Формат priority priority

Режим TACACS Config

timeout

Используйте данную команду в режиме TACACS Configuration, чтобы указать значение таймаута в секундах. Если значение таймаута не определено, будет использоваться глобальное значение. Параметр **timeout** имеет диапазон 1 – 30. Измеряется в секундах.

Формат timeout *timeout*

Режим TACACS Config

show tacacs

Данная команда отображает конфигурацию, статистику и интерфейс-источник клиента TACACS+.

Формат show tacacs [*ip-address*|*hostname*]

Режим Privileged EXEC

Термин	Значение
Host address	IP-адрес или имя хоста настроенного сервера TACACS+.
Port	Номер порта настроенного сервера TACACS+.
TimeOut	Значение таймаута при установке TCP-соединения.
Priority	Предпочтительный порядок серверов TACACS+. Если соединение с сервером неудачно, будет использоваться следующий в порядке приоритета.

show tacacs source-interface

Команда **show tacacs source-interface** в режиме Global Config отображает детали настроенного глобального интерфейса-источника, используемого для клиента TACACS+. IP-адрес выбранного интерфейса используется как адрес источника для всей коммуникации с сервером.

Формат show tacacs source-interface

Режим Privileged EXEC

ПРИМЕР: Пример вывода команды:

```
(Config)# show tacacs source-interface
TACACS Client Source Interface    : loopback 0
TACACS Client Source IPv4 Address  : 1.1.1.1 [UP]
```

5.12. Команды скриптов настройки

Скрипты настройки позволяют создавать текстовые файлы, отображающие текущую конфигурацию системы. Вы можете загружать эти скрипты на ПК или UNIX для редактирования. Затем вы можете загрузить исправленные файлы в систему и применить новую конфигурацию. Один и тот же скрипт можно применить к различным коммутатором без дополнительной настройки (либо с небольшими изменениями).

Используйте команду **show running-config** (см. “show running-config”) для выгрузки текущей конфигурации в виде скрипта. Используйте команду **copy** (см. “copy”) для передачи скрипта с коммутатора или на коммутатор.

Рекомендуется применять скрипты на системах с конфигурацией по умолчанию, однако, не запрещено применять их и на измененные конфигурации.

Скрипты должны соответствовать следующим правилам:

- Расширение файла должно быть ".scr".
- Разрешенный максимум - десять скриптов на коммутатор.
- Совокупный размер всех файлов скриптов на коммутатор не должен превышать 2048 кБ.
- Максимальное количество строк на файл - 2000.

Вы можете использовать однострочные комментарии, чтобы повысить удобство чтения скрипта. Комментарий начинается с восклицательного знака (!). Данный символ может быть расположен в любом месте строки, при этом весь текст справа от символа будет игнорироваться. Любая строка, начинающаяся с «!», воспринимается парсером как комментарий и игнорируется.

Ниже приведен пример скрипта:

```
! Script file for displaying management access show

telnet ! Displays the information about remote connections

! Display information about direct connections

show serial

! End of the script file!
```

ПРИМЕЧАНИЕ: Чтобы указать пустой пароль для пользователя в конфигурационном скрипте, вам нужно указать его как пробел в кавычках. Например чтобы изменить пароль для пользователя jane с пустого пароля на hello, скрипт будет выглядеть следующим образом:

```
users passwd jane
" "
hello
hello
```

script apply

Данная команда применяет команды скрипта на коммутаторе. **scriptname** - имя нужного скрипта.

Формат script apply *scriptname*

Режим Privileged EXEC

script delete

Данная команда удаляет указанный скрипт, параметр **scriptname** - имя скрипта для удаления. **all** - удалить все скрипты, имеющиеся на коммутаторе.

Формат script delete {*scriptname* | all}

Режим Privileged EXEC

script list

Эта команда перечисляет все скрипты, присутствующие на коммутаторе, а также оставшееся свободное пространство.

Формат script list

Режим Privileged EXEC

Термин	Значение
Configuration Script	Имя скрипта.
Size	Privileged EXEC

script show

Данная команда отображает содержимое файла скрипта, название которого задается параметром **scriptname**.

Формат script show *scriptname*

Режим Privileged EXEC

Термин	Значение
Output Format	line *number*: *line contents*

script validate

Эта команда проверяет файл скрипта, анализируя каждую строку в файле скрипта, где **scriptname** - имя скрипта для проверки. Данная функция используется для использования в качестве инструмента для разработки скриптов. Проверка выявляет потенциальные проблемы. Функция не может выявить все возможные проблемы скрипта для любого устройства.

Формат script validate *scriptname*

Режим Privileged EXEC

5.13. Команды Prelogin Banner, System Prompt и Host Name

В этом разделе описаны команды, используемые для настройки системного приглашения и баннера командной строки. Баннером в данном случае называется текст, отображаемый перед входом пользователя в систему.

copy (pre-login banner)

Данная команда включает в себя опции загрузки или выгрузки баннера командной строки на коммутатор либо с коммутатора. Вы можете указать локальные URL с использованием FTP, TFTP, SFTP, SCP либо Xmodem.

ПРИМЕЧАНИЕ: Параметр ip6address также является допустимым параметром для пакетов маршрутизации, поддерживающих протокол IPv6.

По умолчанию none

Формат copy <tftp://<ipaddr>/<filepath>/<filename>> nvram:clibanner copy nvram:clibanner <tftp://<ipaddr>/<filepath>/<filename>>

Режим Privileged EXEC

set prompt

Эта команда изменяет имя приглашения. Имя может содержать до 64 букв и цифр.

Формат set prompt *prompt_string*

Режим Global Config

Hostname

Эта команда устанавливает системное имя хоста. Также она изменяет приглашение. Имя может содержать до 64 букв и цифр (чувствительно к регистру).

Формат hostname *hostname*

Режим Global config

show clibanner

Данная команда отображает текущий баннер командной строки. Баннером в данном случае называется текст, отображаемый перед входом пользователя в систему.

По умолчанию Перед системным приглашением не отображается никакого текста.

Формат show clibanner

Режим Privileged EXEC

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show clibanner
Banner Message configured :
=========================
-------------------------
          TEST
-------------------------
```

set clibanner

Данная команда настраивает баннер командной строки, отображаемый перед входом пользователя в систему.

Формат set clibanner *line*

Режим Global Config

Параметр	Описание
line	Текст баннера, где “” (двойные кавычки) ставятся слева и справа от сообщения. Баннер может содержать до 2000 символов.

no set clibanner

Данная команда сбрасывает настройки баннера командной строки.

Формат no set clibanner

Режим Global Config

6. РАЗДЕЛ: КОМАНДЫ УТИЛИТ

В этом разделе описываются команды утилит, доступные в SMB CLI. The

Раздел состоит из следующих глав:

- Команды AutoInstall
- Команды фильтрации вывода командной строки
- Команды Dual Image
- Команды системной информации и статистики
- Команды журналирования
- Команды почтового сервера и уведомлений по Email
- Команды системных утилит и команды Clear
- Команды SNTP
- Команды часового пояса
- Команды DHCP-сервера
- Команды клиента DNS
- Команды конфликта IP-адресов
- Команды трассировки пакетов обслуживания
- Команда проверки кабеля
- Команды удаленного мониторинга
- Команды приложения статистики

ПРИМЕЧАНИЕ: В данном разделе команды делятся на четыре функциональные группы:

1. Команды Show отображают настройки коммутатора, статистику и прочую информацию.
2. Команды конфигурации вносят изменения в настройки коммутатора. Каждой команде конфигурации соответствует команда информации, показывающая текущие настройки.
3. Команды Copy пересылают или сохраняют конфигурационные или информационные файлы.
4. Команды Clear сбрасывают определенные настройки на заводские значения.

6.1. Команды AutoInstall

Функция AutoInstall активирует автоматическое обновление образа и конфигурации коммутатора. Данная функция обеспечивает конфигурирование и обновление образа коммутатора без участия человека либо с минимальным участием.

AutoInstall включает в себя следующее:

- Загрузка образа с TFTP-сервера с помощью опции DHCP 125. Обновление образа может привести к повышению или понижению версии прошивки коммутатора.
- Автоматическая загрузка файла конфигурации с TFTP-сервера в том случае, если коммутатор загружается без сохраненного файл конфигурации.
- Автоматическая загрузка образа с TFTP-сервера в следующих ситуациях:

- Когда коммутатор загружается без сохраненной конфигурации.
- Когда коммутатор загружается с сохраненной конфигурацией, которая предусматривает включенную функцию AutoInstall.

Когда коммутатор загружается, и файл конфигурации оказывается не найден, производится попытка получить IP-адрес от DHCP-сервера сети. Ответ сервера DHCP включает IP-адрес TFTP-сервера, на котором расположены образ прошивки и файлы конфигурации.

После получения IP-адреса и дополнительной информации с сервера DHCP коммутатор загружает файл образа или файл конфигурации с TFTP-сервера. Загруженный образ устанавливается автоматически. Загруженный файл конфигурации сохраняется в энергонезависимой памяти.

ПРИМЕЧАНИЕ: Автоматическая установка с TFTP-сервера может выполняться на любом IP-интерфейсе, включая сетевой порт, служебный порт и внутренние интерфейсы маршрутизации (если таковые поддерживаются). Для поддержки AutoInstall клиент DHCP функционально включен на служебном порту, если он существует, либо на сетевом порту, если служебный порт отсутствует.

boot autoinstall

Используйте эту команду для функционального запуска или остановки процесса автоустановки на коммутаторе. Данная команда не постоянна и не сохраняется в стартовой или текущей конфигурации.

По умолчанию установлено

Формат boot autoinstall {start| stop}

Режим Privileged EXEC

boot host retrycount

Данная команда устанавливает количество попыток загрузки конфигурационного файла с сервера TFTP.

По умолчанию 3

Формат boot host retrycount 1-3

Режим Privileged EXEC

no boot host retrycount

Данная команда возвращает количество попыток загрузки конфигурационного файла к значению по умолчанию.

Формат no boot host retrycount

Режим Privileged EXEC

boot host dhcp

Данная команда активирует автоматическую установку после следующей перезагрузки. Данная команда не затрагивает текущую конфигурацию автоустановки и сохраняется в NVRAM.

По умолчанию включено

Формат boot host dhcp

Режим Privileged EXEC

no boot host dhcp

Данная команда отключает автоматическую установку после следующей перезагрузки.

Формат no boot host dhcp

Режим Privileged EXEC

boot host autosave

Данная команда автоматически сохраняет загруженный конфигурационный файл, заменяя им имеющийся файл стартовой конфигурации на коммутаторе. При отключенном автосохранении вы должны явно сохранить загруженную конфигурацию в энергонезависимую память командой **write memory or copy system:running-config nvram:startup-config**. Если коммутатор перезагружается, и загруженная конфигурация не была сохранена, процесс начинается процесс автоустановки, если эта функция включена.

По умолчанию отключено

Формат boot host autosave

Режим Privileged EXEC

no boot host autosave

Данная команда отменяет автоматическое сохранение загруженной конфигурации на коммутаторе.

Формат no boot host autosave

Режим Privileged EXEC

boot host autoreboot

Данная команда позволяет коммутатору автоматически перезагружаться после загрузки образа. При включенной автоперезагрузке не требуется какого-либо административного действия для активации образа и перезагрузки коммутатора.

По умолчанию включено

Формат boot host autoreboot

Режим Privileged EXEC

no boot host autoreboot

Данная команда запрещает коммутатору автоматически перезагружаться после того как образ будет загружен при помощи функции автоматической установки.

Формат no boot host autoreboot

Режим Privileged EXEC

erase startup-config

Данная команда стирает текстовый конфигурационный файл, хранимый в энергонезависимой памяти, Если при загрузке коммутатор не может обнаружить конфигурационный файл, процесс автоматической установки начнется немедленно.

Формат erase startup-config

Режим Privileged EXEC

erase factory-defaults

Данная команда стирает текстовый файл заводской конфигурации, хранимый в энергонезависимой памяти,

По умолчанию Отключено

Формат rase factory- defaults

Режим Privileged EXEC

show autoinstall

Данная команда отображает текущее состояние процесса автоматической установки.

Формат show autoinstall

Режим Privileged EXEC

ПРИМЕР: Вывод командной строки для данной команды.

```
(switch) #show autoinstall
AutoInstall Mode..... Stopped
AutoInstall Persistent Mode ..... Disabled
CLI Output Filtering Commands
AutoSave Mode..... Disabled
AutoReboot Mode ..... Enabled
AutoInstall Retry Count..... 3
```

6.2. Команды фильтрации вывода командной строки

show xxx|include “string”

Команда xxx выполняется, и возвращаемая ею информация фильтруется так, что показываются только те строки, которые содержат текст “string”. Другие строки, соответственно, не показываются.

ПРИМЕР: Ниже приведен пример команды.

```
(Routing) #show running-config | include “spanning-tree”
spanning-tree configuration name "00-02-BC-42-F9-33"
spanning-tree bpduguard
spanning-tree bpdufilter default
spanning-tree forceversion  802.1w
```

show xxx|include “string” exclude “string2”

Команда xxx выполняется, и возвращаемая ею информация фильтруется так, что показываются только те строки, которые содержат текст “string” и при этом не содержат

текст “string2”. Другие строки, соответственно, не показываются. Если строка содержит оба образца текста (и include, и exclude), то эта строка также не показывается.

ПРИМЕР: Ниже приведен пример команды.

```
(Routing) #show running-config | include “spanning-tree” exclude “configuration”
spanning-tree bpduguard
spanning-tree bpdufilter default
spanning-tree forceversion 802.1w
```

show xxx|exclude “string”

Команда xxx выполняется, и возвращаемая ею информация фильтруется так, что показываются только те строки, которые НЕ содержат текст “string”. Строки, содержащие “string”, соответственно, не показываются.

ПРИМЕР: Ниже приведен пример команды.

```
(Routing) #show interface 0/1
Packets Received Without Error ..... 0
Packets Received With Error..... 0
Broadcast Packets Received ..... 0
Receive Packets Discarded..... 0
Packets Transmitted Without Errors..... 0
Transmit Packets Discarded..... 0
Transmit Packet Errors ..... 0
Collision Frames..... 0
Time Since Counters Last Cleared..... 281 day 4 hr 9 min 0 sec

(Routing) #show interface 0/1 | exclude “Packets”
CLI Output Filtering Commands
Transmit Packet Errors ..... 0
Collision Frames..... 0
Time Since Counters Last Cleared..... 20 day 21 hr 30 min 9 sec
```

show xxx|begin “string”

Команда xxx выполняется, и возвращаемая ею информация фильтруется так, что показываются все строки, начиная с первой строки, содержащей текст “string”. Предыдущие строки не показываются.

ПРИМЕР: Ниже приведен пример команды.

```
(Routing) #show port all | begin “1/1”
1/1          Enable          Down N/A          Disable N/A
1/2          Enable          Down N/A          Disable N/A
```

1/3	Enable	Down N/A	Disable N/A
1/4	Enable	Down N/A	Disable N/A
1/5	Enable	Down N/A	Disable N/A
1/6	Enable	Down N/A	Disable N/A

(Routing) #

show xxx|section “string”

Команда xxx выполняется, и возвращаемая ею информация фильтруется так, что показываются только те секции кофигурации, которые начинаются со строки содержащей “string” и заканчиваются первым идентификатором конца секции (то есть “exit”).

ПРИМЕР: Ниже приведен пример команды.

(Routing) #show running-config | section “interface 0/1”

interface 0/1 no spanning-tree port mode exit

show xxx|section “string” “string2”

Команда xxx выполняется, и возвращаемая ею информация фильтруется так, что показываются только те секции, которые начинаются с текста “string” и заканчиваются первой строкой содержащей текст “string2”. Может быть отображено несколько таких секций, если они удовлетвояют заданным условиям.

show xxx|section “string” include “string2”

Команда xxx выполняется, и возвращаемая ею информация фильтруется так, что показываются только те секции, которые начинаются с текста “string” и заканчиваются первым идентификатором конца секции (то есть “exit”), и при этом содержат текст “string2”. Команды данного типа также могут включать в себя “exclude” и заданный пользователем идентификатор конца секции.

6.3. Команды Dual Image

ПРИМЕЧАНИЕ: Эти команды доступны только на отдельных платформах, основанных на Linux.

ПО коммутатора поддерживает функцию Dual Image, позволяющую коммутатору иметь два программных образа в постоянной памяти. Вы можете выбрать, какой из образов будет загружен при следующей загрузке. Эта функция позволяет сократить время простоя при обновлении ПО.

delete

Данная команда удаляет резервный образ из постоянной памяти.

Формат delete backup

Режим Privileged EXEC

boot system

Данная команда активирует выбранный образ. Этот образ будет активным при следующей загрузке. Образ, активный в данный момент, отмечается как резервный для последующей перезагрузки. Если указанный файл отсутствует в системе, команда вернет сообщение об ошибке.

Формат boot system {active | backup}

Режим Privileged EXEC

show bootvar

Данная команда отображает информацию о версии и текущем статусе активного и резервного образов. Команда также отображает текстовые описания, относящиеся к образам. Команда отображает состояние активации коммутатора.

Формат show bootvar

Режим Privileged EXEC

filedescr

Данная команда ассоциирует заданное текстовое описание с образом. Существующие описания будут заменены.

Формат filedescr {active | backup} *text-description*

Режим Privileged EXEC

update bootcode

Данная команда обновляет загрузкик (boot loader) коммутатора. Загрузчик для следующей загрузки считывается с активного образа.

Формат update bootcode

Режим Privileged EXEC

6.4. Команды системной информации и статистики

В этом разделе описываются команды, используемые для просмотра информации о системных функциях, компонентах и конфигурациях.

show arp switch

Эта команда отображает содержимое таблицы протокола преобразования адресов (ARP) IP-стека. IP-стек узнает только те записи ARP, которые связаны с интерфейсами управления – сетевыми или сервисными портами. Записи ARP, связанные с интерфейсами маршрутизации, не указываются.

Формат show arp switch

Режим Privileged EXEC

Термин	Значение
IP Address	IP-адрес интерфейса управления или другого устройства в сети управления.

Термин	Значение
MAC Address	Аппаратный MAC-адрес устройства.
Interface	Для сервисного порта вывод – *Management.* Для сетевого порта, вывод - *Unit/slot/port* физического интерфейса.

show eventlog

Данная команда отображает журнал событий, содержащий информацию о системных ошибках. Журнал не очищается после перезагрузки коммутатора.

Формат show eventlog

Режим Privileged EXEC

Термин	Значение
File	Файл, в котором произошло событие.
Line	Номер строки.
Task Id	Task ID события.
Code	Код события.
Time	Время обнаружения события.

ПРИМЕЧАНИЕ: Информация журнала хранится и после перезагрузки коммутатора.

show hardware

Эта команда отображает инвентарную информацию коммутатора.

ПРИМЕЧАНИЕ: Команды **show version** и **show hardware** отображают ту же самую информацию. В будущих версиях ПО команда **show hardware** работать не будет. Описание вывода команды см. в разделе “show version”.

Формат show hardware

Режим Privileged EXEC

show version

Эта команда отображает инвентарную информацию коммутатора.

ПРИМЕЧАНИЕ: В будущих версиях ПО команда **show version** заменит команду **show hardware**.

Формат show version

Режим Privileged EXEC

Термин	Значение
System Description	Текст, используемый в качестве названия этого коммутатора.
Machine Type	Тип оборудования, согласно данным Vital Product Data.
Machine Model	Модель оборудования, согласно данным Vital Product Data.
Серийный номер	Уникальный серийный номер данного коммутатора.
FRU Number	Номер сменного блока (field replaceable unit).
Part Number	Номер детали производителя.
Maintenance Level	Изменения аппаратной платформы, затронувшие программную часть.
Manufacturer	Поле описания производителя.
Burned in MAC Address	Глобально назначенный сетевой адрес.
Software Version	Релизная версия ПО, работающего на коммутаторе в данный момент.
Operating System	Операционная система, работающая на коммутаторе в данный момент.
Network Processing Device	Тип микрокода процессора.
Additional Packages	Дополнительные пакеты, включенные в эту систему.

show platform vpd

Эта команда отображает данные Vital Product Data.

Формат show platform vpd

Режим User Privileged

Отображается следующая информация.

Термин	Значение
Operational Code	Подпись сборки, загруженной на коммутаторе File Name

Термин	Значение
Software Version	Версия релиза, уровня обслуживания и сборки ПО коммутатора.
Timestamp	Время сборки образа

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show platform vpd

Operational Code Image File Name ..... Switch-Ent-esw-xgs4-gto-BL20R-CS-
                                       6AIQHSr3v7m14b35

Software Version..... 3.7.14.35

Timestamp..... Thu Mar  7 14:36:14 IST 2013
```

show interface

Данная команда отображает общую статистику для определенного интерфейса, либо подсчет всего трафика ЦП на основе аргумента.

Формат show interface {unit/slot/port | switchport}

Режим Privileged EXEC

При аргументе **unit/slot/port** отображаются следующие параметры:

Параметры	Значение
Packets Received Without Error	Общее количество пакетов (включая пакеты broadcast и multicast), полученных процессором.
Packets Received With Error	Количество входящих пакетов, содержащих ошибки, не позволяющие их передачу протоколам более высокого уровня.
Broadcast Packets Received	Общее количество полученных пакетов, которые были направлены на широковещательный адрес. Обратите внимание, что многоадресные пакеты при этом не учитываются.
Receive Packets Discarded	Количество входящих пакетов, которые были отклонены, несмотря на то,что в них не было обнаружено ошибок не позволяющих передачу протоколам более высокого уровня. Одной из возможных причин отказа от такого пакета может быть освобождение пространства буфера.
Packets Transmitted Without Error	Общее количество пакетов, переданных из интерфейса.

Параметры	Значение
Transmit Packets Discarded	Количество исходящих пакетов, которые были отклонены, несмотря на то,что в них не было обнаружено ошибок не позволяющих передачу протоколам более высокого уровня. Одной из возможных причин отказа от такого пакета может быть освобождение пространства буфера.
Transmit Packets Errors	Количество исходящих пакетов, которые не могли быть переданы по причине ошибок.
Collisions Frames	Наилучшая оценка общего количества коллизий в этом сегменте Ethernet.
Time Since Counters Last Cleared	Время в днях, часах, минутах и секундах, прошедшее с момента последнего очищения статистики для данного порта.

show interface status

Используйте эту команду, чтобы отобразить информацию об интерфейсах, в том числе описание, состояние порта, скорость и поддержку auto-negotiation. Данная команда схожа с командой **show port all**, но отображает больше информации.

Описание интерфейса настраивается командой **description <name>**. Описание может содержать до 64 символов, которые сокращаются в выводе до 28 символов. Полная форма описания может быть вызвана командой **show port description**. Команда отображает физические интерфейсы, а также интерфейсы LAG и VLAN.

Формат show interface status {*unit/slot/port* | vlan *id* | lag *lag-intf-num* | err-disabled | all}

Режим Privileged EXEC

Поле	Описание
Port	Интерфейс, данные которого приведены в строке.
Name	Имя-описание интерфейса, настраиваемое пользователем.
Link State	Состояние линка. Up или Down.
Physical Mode	Настройки дуплекса и скорости интерфейса.
Physical Status	Указывает скорость порта и дуплексный режим для физического интерфейса. Не показывается для интерфейсов LAG. Если порт в состоянии down, физический статус – unknown.
Media Type	Тип среды передачи данных интерфейса.
Flow Control Status	Режим 802.3x flow control.

Поле	Описание
Flow Control	Настроенный режим 802.3x flow control.

show interface counters

Данная команда отображает ключевые статистические показатели для всех портов (физических/ЦП/port-channel).

Формат show interface counters

Режим Privileged EXEC

Термин	Значение
Port	Интерфейс, данные которого приведены в строке.
InOctects	Общее количество октетов, полученных на интерфейсе.
InUcastPkts	Общее количество одноадресных пакетов, полученных на интерфейсе.
InMcastPkts	Общее количество многоадресных пакетов, полученных на интерфейсе.
Термин	Значение
InBcastPkts	Общее количество широковещательных пакетов, полученных на интерфейсе.
OutOctects	Общее количество октетов, переданных интерфейсом.
OutUcastPkts	Общее количество одноадресных пакетов, переданных интерфейсом.
OutMcastPkts	Общее количество многоадресных пакетов, переданных интерфейсом.
OutBcastPkts	Общее количество широковещательных пакетов, переданных интерфейсом.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show interface counters
```

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
0/1	0	0	0	0

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
0/1	0	0	0	0
0/2	0	0	0	0
0/3	15098	0	31	39
0/4	0	0	0	0
0/5	0	0	0	0
...				
...				
ch1	0	0	0	0
ch2	0	0	0	0
...				
ch64	0	0	0	0
CPU	359533	0	3044	217

Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
0/1	0	0	0	0
0/2	0	0	0	0
0/3	131369	0	11	89
0/4	0	0	0	0
0/5	0	0	0	0
...				
...				
ch1	0	0	0	0
ch2	0	0	0	0
...				
ch64	0	0	0	0
CPU	4025293	0	32910	120

show interface ethernet

Данная команда отображает детальную статистику для определенного интерфейса, либо для всего трафика ЦП на основе аргумента.

Формат show interface ethernet {*unit/slot/port* | switchport | all}

Режим Privileged EXEC

Когда вы указываете значение для **unit/slot/port**, команда возвращает следующую информацию:

Термин	Значение
ts Received	Total Packets Received (Octets) – Общее количество октетов данных (учитывая «плохие» пакеты), полученных в сети (исключая биты кадрирования, включая октеты Frame Check Sequence (FCS)). Этот объект может использоваться как разумная оценка загрузки Ethernet. Если требуется бóльшая точность, должны быть отобраны объекты etherStatsPkt и etherStatsOctets, до и после общего интервала. Результатом этого уравнения является некое значение, которое представляет собой процент загрузки сегмента Ethernet по шкале от 0 до 100 процентов.
	Packets Received 64 Octets – Общее количество принятых пакетов (учитывая «плохие» пакеты), которые имели длину 64 октета (исключая биты кадрирования, но включая октеты FCS).
	Packets Received 65-127 Octets – Общее количество принятых пакетов (учитывая «плохие» пакеты), которые были от 65 до 127 октетов в длину включительно (исключая биты кадрирования, но включая октеты FCS).
ts Received	Packets Received 128-255 Octets – Общее количество принятых пакетов (учитывая «плохие» пакеты), которые были от 128 до 255 октетов в длину включительно (исключая биты кадрирования, но включая октеты FCS).
	Packets Received 256-511 Octets – Общее количество принятых пакетов (учитывая «плохие» пакеты), которые были от 256 до 511 октетов в длину включительно (исключая биты кадрирования, но включая октеты FCS).
	Packets Received 512-1023 Octets – Общее количество принятых пакетов (учитывая «плохие» пакеты), которые были от 512 до 1023 октетов в длину включительно (исключая биты кадрирования, но включая октеты FCS).

Термин	Значение
ts Received	Packets Received 1024-1518 Octets – Общее количество принятых пакетов (учитывая «плохие» пакеты), которые были от 1024 до 1518 октетов в длину включительно (исключая биты кадрирования, но включая октеты FCS).
	Packets Received > 1518 Octets – Общее количество принятых пакетов, которые были длиннее 1518 октетов (исключая биты кадрирования, но включая октеты FCS), и были правильно сформированы.
	Packets RX and TX 64 Octets – Общее количество принятых и переданных пакетов (учитывая «плохие» пакеты), которые имели длину 64 октета (исключая биты кадрирования, но включая октеты FCS).
	Packets RX and TX 65-127 Octets – Общее количество принятых и переданных пакетов (учитывая «плохие» пакеты), которые были от 65 до 127 октетов в длину включительно (исключая биты кадрирования, но включая октеты FCS).
	Packets RX and TX 128-255 Octets – Общее количество принятых и переданных пакетов (учитывая «плохие» пакеты), которые были от 128 до 255 октетов в длину включительно (исключая биты кадрирования, но включая октеты FCS).
	Packets RX and TX 256-511 Octets – Общее количество принятых и переданных пакетов (учитывая «плохие» пакеты), которые были от 256 до 511 октетов в длину включительно (исключая биты кадрирования, но включая октеты FCS).
Packets Received	Packets RX and TX 512-1023 Octets – Общее количество принятых и переданных пакетов (учитывая «плохие» пакеты), которые были от 512 до 1023 октетов в длину включительно (исключая биты кадрирования, но включая октеты FCS).
	Packets RX and TX 1024-1518 Octets – Общее количество принятых и переданных пакетов (учитывая «плохие» пакеты), которые были от 1024 до 1518 октетов в длину включительно (исключая биты кадрирования, но включая октеты FCS).

Термин	Значение
Packets Received	Packets RX and TX 1519-2047 Octets – Общее количество принятых и переданных пакетов, которые были от 1519 до 2047 октетов в длину включительно (исключая биты кадрирования, но включая октеты FCS), и были правильно сформированы.
	Packets RX and TX 1523-2047 Octets – Общее количество принятых и переданных пакетов, которые были от 1523 до 2047 октетов в длину включительно (исключая биты кадрирования, но включая октеты FCS), и были правильно сформированы.
	Packets RX and TX 2048-4095 Octets – Общее количество принятых и переданных пакетов, которые были от 2048 до 4095 октетов в длину (исключая биты кадрирования, но включая октеты FCS), и были правильно сформированы.
	Packets RX and TX 4096-9216 Octets – Общее количество принятых и переданных пакетов, которые были от 4096 до 9216 октетов в длину включительно (исключая биты кадрирования, но включая октеты FCS), и были правильно сформированы.
Packets Received Successfully	Total Packets Received Without Error – Общее количество пакетов, полученных без ошибок.
	Unicast Packets Received – Количество одноадресных пакетов из подсети, переданных протоколам высшего уровня.
	Multicast Packets Received – Общее количество полученных правильно сформированных многоадресных пакетов. Обратите внимание, что в это количество не входят широковещательные пакеты.
	Broadcast Packets Received – Общее количество полученных правильно сформированных широковещательных пакетов. Обратите внимание, что многоадресные пакеты при этом не учитываются.

Термин	Значение
Receive Packets Discarded	Количество входящих пакетов, которые были отклонены несмотря на то, что в них не было обнаружено ошибок, не позволяющих передачу протоколам более высокого уровня. Одной из возможных причин отказа от такого пакета может быть освобождение пространства буфера.
Packets Received with MAC Errors	Total Packets Received with MAC Errors – общее количество входящих пакетов с ошибкой, которая помешала их передаче протоколам более высокого уровня.
	Jabbers Received – Общее количество полученных пакетов, длина которых превышает 1518 октетов (исключая кадрирующие биты, но включая октеты FCS), и имела либо неверную Frame Check Sequence (FCS) с целым числом октетов (FCS Error), либо неверную FCS с нецелым число октетов (Alignment Error). Обратите внимание, что данное определение термина «jabber» отличается от определения в IEEE-802.3, разделах 8.2.1.5 (10BASE5) и 10.3.1.4 (10BASE2). Эти документы определяют jabber как состояние, когда какой-либо пакет превышает 20 мс. Допустимый диапазон обнаружения jabber составляет от 20 до 150 мс.
	Fragments/Undersize Received – Общее количество принятых пакетов, которые имели длину менее 64 октетов (исключая кадрирующие биты, но включая октеты FCS).
	Alignment Errors – Общее количество принятых пакетов, имевших длину (исключая кадрирующие биты, но включая октеты FCS) между 64 и 1518 октетами включительно, но имевших при этом неверную Frame Check Sequence (FCS) с нецелым количеством октетов.
	FCS Errors – Общее количество принятых пакетов, имевших длину (исключая кадрирующие биты, но включая октеты FCS) между 64 и 1518 октетами включительно, но имевших при этом неверную Frame Check Sequence (FCS) с целым количеством октетов.
	Overruns – Общее количество фреймов, отклоненных по причине перегруженности порта входящими пакетами.

Термин	Значение
Received Packets Not Forwarded	Total Received Packets Not Forwarded – Количество принятых верных фреймов, которые были отброшены (другими словами, отфильтрованы) процессом пересылки.
	802.3x Pause Frames Received – Количество кадров MAC control, полученных на этом интерфейсе, с кодом операции, указывающим операцию PAUSE. Счетчик не инкрементируется, если интерфейс работает в полудуплексном режиме.
	Unacceptable Frame Type – Количество фреймов, отброшенных по причине неприемлемого типа.
Packets Transmitted Octets	Total Packets Transmitted (Octets) – Общее количество октетов данных (включая «плохие» пакеты), полученных в сети (исключая кадрирующие биты, но включая октеты FCS). Этот объект может использоваться как разумная оценка загрузки Ethernet. Если требуется бóльшая точность, должны быть отобраны объекты etherStatsPkt и etherStatsOctets, до и после общего интервала.
	Packets Transmitted 64 Octets – Общее количество переданных пакетов (учитывая «плохие» пакеты), которые имели длину 64 октета (исключая биты кадрирования, но включая октеты FCS).
	Packets Transmitted 65-127 Octets – Общее количество переданных пакетов (учитывая «плохие» пакеты), которые были от 65 до 127 октетов в длину включительно (исключая биты кадрирования, но включая октеты FCS).
	Packets Transmitted 128-255 Octets – Общее количество переданных пакетов (учитывая «плохие» пакеты), которые были от 128 до 255 октетов в длину включительно (исключая биты кадрирования, но включая октеты FCS).
	Packets Transmitted 256-511 Octets – Общее количество переданных пакетов (учитывая «плохие» пакеты), которые были от 256 до 511 октетов в длину включительно (исключая биты кадрирования, но включая октеты FCS).

Термин	Значение
Packets Transmitted Octets	Packets Transmitted 512-1023 Octets – Общее количество переданных пакетов (учитывая «плохие» пакеты), которые были от 512 до 1023 октетов в длину включительно (исключая биты кадрирования, но включая октеты FCS).
	Packets Transmitted 1024-1518 Octets – Общее количество переданных пакетов (учитывая «плохие» пакеты), которые были от 1024 до 1518 октетов в длину включительно (исключая биты кадрирования, но включая октеты FCS).
	Transmitted > 1518 Octets – Общее количество переданных пакетов, которые были длиннее 1518 октетов (исключая биты кадрирования, но включая октеты FCS), и были правильно сформированы.
	Max Frame Size – Максимальный размер поля Info (без MAC), которое этот порт будет принимать или передавать.
Packets Transmitted Successfully	Total Packets Transmitted Successfully– Количество фреймов, переданных этим портом в его сегмент.
	Unicast Packets Transmitted – Общее количество пакетов, запрошенных протоколами более высокого уровня для отправки на индивидуальный адрес в подсети, включая те, которые были отброшены или не отправлены.
	Multicast Packets Transmitted – Общее количество пакетов, запрошенных протоколами более высокого уровня для отправки на групповой адрес в подсети, включая те, которые были отброшены или не отправлены.
	Broadcast Packets Transmitted – Общее количество пакетов, запрошенных протоколами более высокого уровня для отправки на широковещательный адрес в подсети, включая те, которые были отброшены или не отправлены.
Transmit Packets Discarded	Количество исходящих пакетов, которые были отклонены несмотря на то,что в них не было обнаружено ошибок, не позволяющих передачу протоколам более высокого уровня. Одной из возможных причин отказа от такого пакета может быть освобождение пространства буфера.

Термин	Значение
Transmit Errors	Total Transmit Errors – Сумма одиночных, множественных и черезмерных коллизий.
	FCS Errors – Общее количество переданных пакетов, имевших длину (исключая кадрирующие биты, но включая октеты FCS) между 64 и 1518 октетами включительно, но имевших при этом неверную Frame Check Sequence (FCS) с нецелым количеством октетов.
	Underrun Errors – Общее количество фреймов, отброшенных по причине опустошения передающего буфера FIFO во время передачи.
Transmit Discards	Total Transmit Packets Discards – Суммы фреймов, отброшенных из-за коллизий: одиночных, множественных и черезмерных.
	Single Collision Frames – Количество фреймов, успешно переданных на определенный интерфейс, для которых передача была заблокирована единственной коллизией.
	Multiple Collision Frames – Количество фреймов, успешно переданных на определенный интерфейс, для которых передача была заблокирована несколькими коллизиями.
	Excessive Collisions – Количество фреймов, передача которых на определенный интерфейс завершилась неудачно по причине черезмерных коллизий.
	Port Membership Discards – Количество фреймов, отбрасываемых при выходе для этого порта из-за включенной исходящей фильтрации.
Protocol Statistics	802.3x Pause Transmitted – Количество кадров MAC Control, переданных этим интерфейсом, с кодом операции, указывающим операцию PAUSE. Счетчик не инкрементируется, если интерфейс работает в полудуплексном режиме.
	GVRP PDUs Received – Количество GVRP PDU, полученных на уровне GARP.

Термин	Значение
Protocol Statistics	GVRP PDUs Transmitted – Количество GVRP PDU, переданных на уровне GARP.
	GVRP Failed Registrations – Количество безуспешных попыток регистрации GVRP.
	GMRP PDUs Received – Количество GMRP PDU, полученных на уровне GARP.
	GMRP PDUs Transmitted – Количество GMRP PDU, переданных на уровне GARP.
	GMRP Failed Registrations – Количество безуспешных попыток регистрации GMRP.
	STP BPDUs Transmitted – Количество отправленных BPDU протокола Spanning Tree.
	STP BPDUs Received – Количество принятых BPDU протокола Spanning Tree.
	RST BPDUs Transmitted – Количество отправленных BPDU протокола Rapid Spanning Tree.
	RSTP BPDUs Received – Количество принятых BPDU-протокола Rapid Spanning Tree Protocol.
	MSTP BPDUs Transmitted – Количество отправленных BPDU-протокола Multiple Spanning Tree.
	MSTP BPDUs Received – Количество принятых BPDU-протокола Multiple Spanning Tree.
Dot1x Statistics	EAPOL Frames Transmitted – Количество фреймов EAPOL любого типа, переданных этим аутентификатором.
	EAPOL Start Frames Received – Количество действительных стартовых фреймов EAPOL, полученных этим аутентификатором.

Термин	Значение
Time Since Counters Last Cleared	Время в днях, часах, минутах и секундах, прошедшее с момента последнего очищения статистики на данном порту.

При использовании ключевого слова **switchport** появляется следующая информация.

Термин	Значение
Packets Received Without Error	Общее количество пакетов (включая широковещательные и многоадресные), полученных процессором.
Broadcast Packets Received	Общее количество полученных пакетов, которые были направлены на широковещательный адрес. Обратите внимание, что многоадресные пакеты при этом не учитываются.
Packets Received With Error	Общее количество пакетов с ошибками (влкючая широковещательные и многоадресные пакеты), полученные процессором.
Packets Transmitted without Errors	Общее количество пакетов, переданных из интерфейса.
Broadcast Packets Transmitted	Общее количество пакетов, запрошенных протоколами более высокого уровня для отправки на широковещательный адрес, включая те, которые были отброшены или не отправлены.
Transmit Packet Errors	Количество исходящих пакетов, которые не могли быть переданы по причине ошибок.
Time Since Counters Last Cleared	Время в днях, часах, минутах и секундах, прошедшее с момента последнего очищения статистики для данного коммутатора.

При использовании ключевого слова all появляется следующая информация.

Термин	Значение
Port	Идентификатор интерфейса.
Bytes Tx	Общее количество байт, переданных интерфейсом.
Bytes Rx	Общее количество байт, полученных интерфейсом.

Термин	Значение
Packets Tx	Общее количество пакетов, переданных интерфейсом.
Packets Rx	Общее количество пакетов, полученных интерфейсом.

show interface ethernet switchport

Данная команда отображает информацию о схеме private VLAN для интерфейсов коммутатора.

Формат show interface ethernet *interface-id* switchport

Режим Privileged EXEC

Параметр	Описание
interface-id	Unit/slot/port коммутатора.

Команда отображает следующую информацию.

Термин	Значение
Private-vlan hostassociation	Соответствие VLAN для private-VLAN хост портов.
Private-vlan mapping	Соответствие VLAN для private-VLAN смешаных портов.

show interface lag

Данная команда отображает информацию о конфигурации определенного интерфейса LAG.

Формат show interface lag *lag-intf-num*

Режим Privileged EXEC

Параметры	Значение
Packets Received Without Error	Общее количество пакетов (включая широковещательные и многадресные пакеты), полученных на интерфейсе LAG.
Packets Received With Error	Количество входящих пакетов, содержащих ошибки, не позволяющие их передачу протоколам более высокого уровня.

Параметры	Значение
Broadcast Packets Received	Общее количество полученных пакетов, которые были направлены на широковещательный адрес. Обратите внимание, что многоадресные пакеты при этом не учитываются.
Receive Packets Discarded	Количество входящих пакетов, которые были отклонены несмотря на то, что в них не было обнаружено ошибок, не позволяющих передачу протоколам более высокого уровня. Одной из возможных причин отказа от такого пакета может быть освобождение пространства буфера.
Packets Transmitted Without Error	Общее количество пакетов, переданных из LAG.
Transmit Packets Discarded	Количество исходящих пакетов, которые были отклонены несмотря на то,что в них не было обнаружено ошибок, не позволяющих передачу протоколам более высокого уровня. Одной из возможных причин отказа от такого пакета может быть освобождение пространства буфера.
Transmit Packet Errors	Количество исходящих пакетов, которые не могли быть переданы по причине ошибок.
Collisions Frames	Наилучшая оценка общего количества коллизий в этом сегменте Ethernet.
Time Since Counters Last Cleared	Время в днях, часах, минутах и секундах, прошедшее с момента последнего очищения статистики для этого LAG.

show fiber-ports optical-transceiver

Данная команда отображает диагностическую информацию SFP, такую как температура, напряжение, ток, входная мощность, выходная мощность, количество ошибок при передаче и LOS. Значения выводятся из диагностической таблицы SFP A2 с использованием интерфейса I^2C.

Формат show fiber-ports optical-transceiver {all | *unit/slot/port*}

Режим Privileged EXEC

Поле	Описание
Temp	Внутренняя температура трансивера.
Voltage	Внутреннее напряжение питания трансивера.

Поле	Описание
Current	Ток смещения трансмиттера.
Output Power	Измеренная оптическая мощность, относительно 1 мВт.
Input Power	Измеренная полученная оптическая мощность, относительно 1 мВт.
TX Fault	Ошибка трансмиттера.
Поле	Описание
LOS	Потеря сигнала

ПРИМЕР: Ниже приведен пример выполнения команды:

```
(Switch) #show fiber-ports optical-transceiver all
                                      Output   Input
Port     Temp    Voltage   Current   Power    Power    TX      LOS
         [C]     [Volt]    [mA]      [dBm]    [dBm]    Fault
----------------------------------------------------------------------------
0/49     39.3    3.256     5.0       -2.234   -2.465   No      No
0/50     33.9    3.260     5.3       -2.374   -40.000  No      Yes
0/51     32.2    3.256     5.6       -2.300   -2.897   No      No
```

show fiber-ports optical-transceiver-info

Данная команда отображает информацию SFP, относящуюся к производителю устройства, а именно: название производителя, серийный номер SFP и номер детали. Значения выводятся из таблицы SFP A0 с использованием интерфейса I^{2}C.

Формат show fiber-ports optical-transceiver-info {all | *slot/port*}

Режим Privileged EXEC

Поле	Описание
Vendor Name	Поле емкостью в 16 символов ASCII, выравненное по левому краю и сдвинутое вправо при помощи пробелов ASCII (20h). Данная строка должна представлять собой полное название компании-производителя, общепринятое сокращение этого названия, код SCSI либо биржевой код компании-производителя.

Поле	Описание
Length (50um, OM2)	Это значение указывает длину линии, поддерживаемую трансивером, при работе в соответствии с применимыми стандартами с использованием 50-микронного многомодового волокна OM2 [500 МГц*км на 850 нм]. Нулевое значение говорит о том, что трансивер не поддерживает 50-микронное многомодовое волокно, либо длину канала необходимо выяснить из технологии трансивера.
Length (62.5um, OM1)	Это значение указывает длину линии, поддерживаемую приемопередатчиком, при работе в соответствии с применимыми стандартами с использованием 62,5-микронного многомодового волокна OM1 [200 МГц*км на 850 нм, 500 МГц*км на 1310 нм]. Нулевое значение говорит о том, что трансивер не поддерживает 62,5-микронное многомодовое волокно, либо длину канала необходимо выяснить из технологии трансивера
Vendor SN	Серийный номер производителя. Представляет собой поле емкостью в 16 символов, содержащее символы ASCII, выравненное по левому краю и сдвинутое вправо при помощи пробелов ASCII (20h), определяющее серийный номер производителя для трансивера. Нулевое значение говорит о том, что серийный номер производителя не указан.
Vendor PN	Номер детали производителя (vendor PN) 16-байтное поле, содержащее символы ASCII, выравненное по левому краю и сдвинутое вправо при помощи пробелов ASCII (20h). Определяет номер детали и название продукта. Нулевое значение говорит о том, что номер детали производителя не указан.
BR, nominal	Номинальная скорость передачи данных (BR) указывается в единицах 100 МБод, округленная до ближайшего 100 МБод. Величина включает в себя те биты, которые необходимы для кодирования и разграничения сигнала, а также биты, содержащие информацию о данных. Нулевое значение говорит о том, что скорость передачи данных не задана и должна быть определена исходя из технологии трансивера. Фактическая скорость передачи информации будет зависеть от кодирования данных.
Vendor Rev	Номер ревизии производителя (vendor rev), содержащий символы ASCII, выровненный по левому краю и сдвинутый вправо при помощи пробелов ASCII (20h). Определяет ревизию продукта. Нулевое значение говорит о том, что номер ревизии не указан.

ПРИМЕР: Ниже приведен пример выполнения команды:

```
(Switch) #show fiber-ports optical-transceiver-info all
```

Port	Vendor Name	Link Length 50um [m]	Link Length 62,5um [m]	Serial Number	Part Number	Nominal Bit Rate [Mbps]	Rev
0/49	Switch	8	3	2018414	761	10300	10
0/51	Switch	8	3	2018472	761	10300	10
0/52	Switch	8	3	2018501	761	10300	10

show mac-addr-table

Данная команда выводит записи таблицы коммутации (FDB). Эти записи используются функцией прозрачного моста для определения того, каким образом перенаправить полученный фрейм.

Ключевое слово all или отсутствие параметров - показать всю таблицу. Введите MAC-адрес и VLAN ID, чтобы отобразить записи таблицы для требуемого MAC-адреса на указанном VLAN. Параметр *count* - показать сводную информацию о таблице коммутации. Параметр **interface unit/slot/port** - показать MAC-адрес на указанном интерфейсе.

Для указания интерфейса LAG вместо **unit/slot/port** можно использовать **lag-intf-num**. Также для определения интефейса LAG можно использовать **lag-intf-num**, где **lag-intf-num** - номер порта LAG. Параметр *vlan vlan_id* отображает информацию о MAC-адресах в указанной VLAN.

Формат show mac-addr-table [{*macaddr vlan_id* | all | count | interface {*unit/slot/port* | lag *lag-id* | vlan *vlan_id*} | vlan *vlan_id*}]

Режим Privileged EXEC

Следующая информация отображается, если вы не введете параметр, ключевое слово «all», MAC-адрес либо VLAN ID.

Термин	Значение
VLAN ID	VLAN, в которой изучен MAC-адрес.
MAC Address	Одноадресный MAC-адрес, для которого коммутатор имеет информацию о перенаправлении или фильтрации. Формат - 6 двухзначных шестнадцатеричных чисел, разделенных двоеточиями, например 01:23:45:67:89:AB.
Interface	Порт, через который был изучен адрес.
Interface Index	Данный объект показывает индекс интерфейса таблицы интерфейсов, ассоциированной с этим портом.

Термин	Значение
Status	Статус этой записи. Значения: • Static—Значение соответствующего экземпляра было добавлено системой или пользователем, когда был определен статический фильтр MAC. Он не может быть переучен. • Learned—Значение соответствующего экземпляра было изучено путем наблюдения MAC-адресов источника входящего трафика и используется в настоящее время. • Management—Значение соответствующего экземпляра (системного MAC-адреса) также является значением существующего экземпляра dot1dStaticAddress. Он идентифицируется интерфейсом 0/1. и в настоящее время используется при включении VLAN для маршрутизации. • Self—Значение соответствующего экземпляра - это адрес одного из физических интерфейсов коммутатора (собственный MAC-адрес системы). • GMRP Learned—Значение соответствующей информации было получено с помощью GMRP и применяется к многоадресной рассылке. • Other—Значение соответствующего экземпляра не относится к одной из других категорий.

Если вы введете **vlan vlan_id**, будут показаны только поля MAC-адреса, интерфейса и состояния. Если вы введете параметр **interface unit/slot/port**, то в дополнение к полям MAC-адреса и состояния появится поле VLAN ID.

Следующая информация отображается, если вы введете параметр *count*:

Термин	Значение
Dynamic Address count	Количество MAC-адресов в таблице коммутации, которые были автоматически изучены.
Static Address (User-defined) count	Количество MAC-адресов в таблице коммутации, введенных вручную пользователем.
Total MAC Addresses in use	Количество MAC-адресов, находящихся в настоящее время в таблице коммутации.
Total MAC Addresses available	Количество MAC-адресов, которое способна поддерживать таблица коммутации.

process cpu threshold

Данная команда настраивает пороги использования ЦП. Верхний и нижний пороги и указываются в виде определенного процента от ресурсов ЦП. Мониторинг использования может быть настроен от 5 секунд до 86400 секунд, умноженные на 5 секунд. Пороговое значение использования ЦП сохраняется после перезагрузки коммутатора. Настраивать нижний порог необязательно. Если значение нижнего порога не настроено, оно считается совпадающим со значением верхнего порога.

Формат process cpu threshold type total rising *1-100* interval

Режим Global Config

Параметр	Описание
rising threshold	Верхний порог – процентное значение ресурсов ЦП, превышение которого на указанный временной интервал («rising interval») вызывает уведомление. Диапазон - от 1 до 100. Значение по умолчанию - 0 (отключено).
rising interval	Длительность превышения ресурсов ЦП в секундах, которая должна повлечь за собой отправку уведомления. Диапазон - от 5 до 86400. Значение по умолчанию - 0 (отключено).
falling threshold	Нижний порог - процентное значение ресурсов ЦП. Уведомление происходит, когда использование ЦП падает ниже данного значения на указанный временной интервал. Диапазон - от 1 до 100. Значение по умолчанию - 0 (отключено). Уведомление происходит в том случае, когда общий коэффициент использования ЦП падает ниже этого уровня в течение периода времени, указанного в настройках. Уведомление о нижнем пороговом значении падения производится только в том случае, если ранее было получено уведомление о верхнем пороговом значении. Нижнее пороговое значение всегда должно быть ниже верхнего. Не допускается нижнее пороговое значение, превышающее верхнее.
falling interval	Длительность использования ресурсов ЦП ниже порогового значения (в секундах), которая должна повлечь за собой отправку уведомления. Диапазон - от 5 до 86400. Значение по умолчанию - 0 (отключено).

show process app-list

Данная команда отображает пользовательские и системные приложения.

Формат show process app-list

Режим Privileged EXEC

Параметр	Описание
ID	Идентификатор приложения.
Name	Имя, определяющее процесс.
PID	Число, которое используется ПО для идентификации процесса.
Admin Status	Административный статус процесса.
Auto Restart	Указывает на то, перезапускается ли процесс автоматически после остановки.
Running Status	Указывает на то, запущен или остановлен процесс в настоящий момент.

ПРИМЕР: Вывод командной строки для данной команды.

```
                                                    Admin                    Auto
Running ID      Name            PID                 Status      Restart      Status
-------------------------------------------------------------------------------
1               dataplane       15309               Enabled     Disabled     Running
2               switchdrvr      15310               Enabled     Disabled     Running
3               syncdb          15314               Enabled     Disabled     Running
4               lighttpd        18718               Enabled     Enabled      Running
5               syncdb-test     0                   Disabled    Disabled     Stopped
6               proctest        0                   Disabled    Enabled      Stopped
7               user.start      0                   Enabled     Disabled     Stopped
```

show process app-resource-list

Данная команда отображает настроенные и используемые ресурсы для каждого приложения.

Формат show process app-resource-list

Режим Privileged EXEC

Параметр	Описание
ID	Идентификатор приложения.
Name	Имя, определяющее процесс.
PID	Число, которое используется ПО для идентификации процесса.

Параметр	Описание
Memory Limit	Максимальное количество памяти, которое может получить процесс.
CPU Share	Максимальный процент ресурсов ЦП, который может получить процесс.
Memory Usage	Количество памяти, используемое процессором в настоящее время.
Max Mem Usage	Максимальное количество памяти, выделявшееся на процесс с момента его запуска.

(Routing) #show process app-resource-list

ID	Name	PID	Memory Limit	CPUShare	Memory Usage	Max Mem Usage
1	switchdrvr	251	Unlimited	Unlimited	380 MB	381 MB
2	syncdb	252	Unlimited	Unlimited	0 MB	0 MB
3	syncdb-test	0	Unlimited	Unlimited	0 MB	0 MB
4	proctest	0	10 MB	20 %	0 MB	0 MB
5	utelnetd	0	Unlimited	Unlimited	0 MB	0 MB
6	lxshTelnetd	0	Unlimited	Unlimited	0 MB	0 MB
7	user.start	0	Unlimited	Unlimited	0 MB	0 MB

show process cpu

Данная команда предоставляет информацию о процентном соотношении использования ресурсов ЦП различными задачами.

ПРИМЕЧАНИЕ: Задачи, загружающие ресурсы ЦП, не ограничиваются обработкой траффика.

Формат show process cpu [*1-n* | all]

Режим Privileged EXEC

Ключевое слово	Описание
Free	Свободная память всей системы

Ключевое слово	Описание
Alloc	Выделенная память всей системы (не включая кэш и пространство, используемое системой)
Pid	Идентификатор процесса или цепочки процессов
Name	Имя процесса или цепочки процессов
5Secs	Статистика использования ЦП за 5-секундный интервал
60Secs	Статистика использования ЦП за 60-секундный интервал
300Secs	Статистика использования ЦП за 300-секундный интервал
Total CPU Utilization	Общий процент использования ЦП в пределах указанного окна в 5, 60 или 300 секунд.

ПРИМЕР: Выполнение команды с использованием Linux.

```
(Routing) #show process cpu
Memory          Utilization     Report          status
Bytes           ------          ---------       free
106450944       alloc           423227392       CPU
Utilization:
PID     Name                                5 Secs      60 Secs     300 Secs
--------------------------------------------------------------------------------
765     _interrupt_thread                   0.00%       0.01%       0.02%
767     bcmL2X.0                            0.58%       0.35%       0.28%
768     bcmCNTR.0                           0.77%       0.73%       0.72%
773     bcmRX                               0.00%       0.04%       0.05%
786     cpuUtilMonitorTask                  0.19%       0.23%       0.23%
834     dot1s_task                          0.00%       0.01%       0.01%
810     hapiRxTask                          0.00%       0.01%       0.01%
805     dtlTask                             0.00%       0.02%       0.02%
863     spmTask                             0.00%       0.01%       0.00%
894     ip6MapLocalDataTask                 0.00%       0.01%       0.01%
908     RMONTask                            0.00%       0.11%       0.12%
--------------------------------------------------------------------------------
Total   CPU Utilization                      1.55%       1.58%       1.50%
```

show process proc-list

Это приложение отображает процессы, запущенные приложениями, которые, в свою очередь, были созданы Менеджером Процессов.

Формат show process proc-list

Режим Privileged EXEC

Параметр	Описание
PID	Число, которое используется ПО для идентификации процесса.
Process Name	Имя, определяющее процесс.
Application ID-Name	Идентификатор приложения и его связанное имя.
Child	Указывает, запустил ли этот процесс дочерний процесс.
VM Size	Размер виртуальной памяти.
VM Peak	Максимальный объем виртуальной памяти, использованный данным процессом за указанное время.
FD Count	Дескрипторы файла, подсчитанные для процесса.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show process proc-list
```

PID	Process Name	Application ID-Name	Chld	VM Size (KB)	VM Peak (KB)	FD Count
15260	procmgr	0-procmgr	No	1984	1984	8
15309	dataplane	1-dataplane	No	293556	293560	11
15310	switchdrvr	2-switchdrvr	No	177220	177408	57
15314	syncdb	3-syncdb	No	2060	2080	8
18718	lighttpd	4-lighttpd	No	5508	5644	11
18720	lua_magnet	4-lighttpd	Yes	12112	12112	7
18721	lua_magnet	4-lighttpd	Yes	25704	25708	7

show running-config

Используйте эту команду для отображения или захвата текущей настройки различных пакетов протоколов, поддерживаемых коммутатором. Эта команда отображает или захватывает команды с настройками и конфигурациями, которые отличаются от значений

по умолчанию. Чтобы отображать или захватывать команды, совпадающие с настройками и конфигурациями по умолчанию, добавьте опцию **all**.

ПРИМЕЧАНИЕ: **Show running-config** не отображает пользовательский пароль, даже если он не совпадает с паролем по умолчанию.

Команда возвращает результат в формате скрипта, который может использоваться для настройки других коммутаторов той же конфигурацией. Если приведено опциональное значение **scriptname** с расширением файла “.scr”, результат перенаправляется в файл скрипта.

ПРИМЕЧАНИЕ: Если команда **show running-config** запускается через консоль, удаленный доступ к коммутатору (например, по Telnet) приостанавливается на время генерации и отображения вывода команды.

ПРИМЕЧАНИЕ: Если вы используете текстовый файл конфигурации, команда **show running-config** отображает только настроенные физические интерфейсы (т. е. если какой-либо интерфейс содержит только конфигурацию по умолчанию, его в выводе команды **show running-config** не будет). Это верно для любого режима конфигурации, который не содержит ничего, кроме конфигурации по умолчанию. Таким образом, если следом за командой входа в определенный режим конфигурации сразу же последует команда выхода, эти команды не будут отмечены в выводе (и, соответственно, в конфигурационном файле, если таковой создается на основе данной вывода команды **show running-config**).

Используйте следующие кнопки для навигации в выводе команды.

Клавиша	Действие
Enter	На одну строку вперед.
Пробел	На одну страницу вперед.
q	Прервать вывод и выйти в командную строку.

Обратите внимание на то, что внизу экрана вывода отображаются слова --More-- or (q)uit, пока не будет достигрут конец вывода.

Формат show running-config [all | scriptname]

Режим Privileged EXEC

show running-config interface

Данная команда отображает текущую конфигурацию указанного интерфейса. Может применяться к физическим интерфейсам, LAG, петлям, туннелям и интерфейсам VLAN.

Формат show running-config interface {*interface* | lag {*lag-intf-num*} | vlan {*vlan-id*}}

Режим Privileged EXEC

Параметр	Описание
interface	Текущая конфигурация указанного интерфейса.
lag-intf-num	Текущая конфигурация интерфейса LAG.

Параметр	Описание
Параметр	Описание
vlan-id	Текущая конфигурация маршрутизируемого интерфейса VLAN.

По команде отображается следующая информация.

Параметр	Описание
unit|slot|port	Доступ к интерфейсу в формате unit/slot/port.
lag	Отображение текущей конфигурации указанного интерфейса LAG.
vlan	Отображение текущей конфигурации указанного маршрутизируемого интерфейса VLAN.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show running-config interface 0/1
!Current Configuration:
!
interface 0/1
addport 3/1
exit
(Routing) #
```

show

Данная команда отображает содержимое текстовых конфигурационных файлов в командной строке. Текстовые конфигурационные файлы (конфигурация при загрузке, резервная и заводские значения) хранятся на flash в сжатом виде. При выполнении данной команды файлы распаковываются.

Формат show { startup-config | backup-config | factory-defaults }

Режим Privileged EXEC

Параметр	Описание
startup-config	Показать конфигурацию при загрузке.
backup-config	Показать резервную конфигурацию.
factory-defaults	Показать конфигурацию при сбросе на значения по умолчанию.

ПРИМЕР: Просмотр конфигурации при загрузке.

```
(Routing) #show startup-config
```

```
!Current Configuration:
!
!System Description "Switch 56218 Development System - 50 GE, 2 HGL, R.5.5.1, Linux 2.6.34.6"
!System Software Version "R.5.5.1"
!System Up Time          "0 days 2 hrs 47 mins 59 secs"
!Cut-through mode is configured as disabled
!Additional Packages     Switch QOS,Switch IPv6 Management,Switch Stacking,Switch Routing
!Current SNTP Synchronized Time: SNTP Client Mode Is Disabled
! vlan database
exit
configure
stack
member 2 4
exit
slot 2/0 5
set slot power 2/0
no set slot disable 2/0
line console
exit
line telnet
exit
--More-- or (q)uit
line ssh
exit
!
exit
(Routing) #
```

ПРИМЕР: Просмотр резервной конфигурации.

```
(Routing) #show backup-config
!Current Configuration:
!
!System Description "Switch 56218 Development System - 50 GE, 2 HGL, R.5.5.1, Linux 2.6.34.6"
!System Software Version "R.5.5.1"
!System Up Time          "0 days 2 hrs 47 mins 59 secs"
!Cut-through mode is configured as disabled
```

!Additional Packages Switch QOS,Switch IPv6 Management,Switch Stacking,Switch Routing

!Current SNTP Synchronized Time: SNTP Client Mode Is Disabled

!

vlan

database

exit

configure

stack

member 2 4

exit

slot

2/0 5

set slot power 2/0

no set slot disable 2/0

line console

exit

line telnet

exit line ssh

exit

!

exit

(Routing) #

ПРИМЕР: Просмотр конфигурации по умолчанию.

(Routing) #show factory-defaults

!Current Configuration:

!

!System Description "Switch 56218 Development System - 50 GE, 2 HGL, R.5.5.1, Linux 2.6.34.6"

!System Software Version "R.5.5.1"

!System Up Time "0 days 2 hrs 47 mins 59 secs"

!Cut-through mode is configured as disabled

!Additional Packages Switch QOS,Switch IPv6 Management,Switch Stacking,Switch Routing

!Current SNTP Synchronized Time: SNTP Client Mode Is Disabled

!

vlan

database

exit

configure
stack
member 2 4
exit
slot 2/0 5
set slot power 2/0
no set slot disable 2/0
line console
exit
line telnet
exit
--More-- or (q)uit
line ssh
exit
!
exit
(Routing) #

dir

Используйте эту команду, чтобы поросмотреть список файлов в каталоге /mnt/switch во flash-памяти.

Формат dir

Режим Privileged EXEC

(Routing) #dir

0	drwx	2048	May	09 2002 16:47:30	.
0	drwx	2048	May	09 2002 16:45:28	..
0	-rwx	592	May	09 2002 14:50:24	slog2.txt
0	-rwx	72	May	09 2002 16:45:28	boot.dim
0	-rwx	0	May	09 2002 14:46:36	olog2.txt
0	-rwx	13376020	May	09 2002 14:49:10	image1
0	-rwx	0	Apr	06 2001 19:58:28	fsyssize
0	-rwx	1776	May	09 2002 16:44:38	slog1.txt
0	-rwx	356	Jun	17 2001 10:43:18	crashdump.ctl
0	-rwx	1024	May	09 2002 16:45:44	sslt.rnd
0	-rwx	14328276	May	09 2002 16:01:06	image2

```
0   -rwx   148      May    09 2002 16:46:06   hpc_broad.cfg
0   -rwx   0        May    09 2002 14:51:28   olog1.txt
0   -rwx   517      Jul    23 2001 17:24:00   ssh_host_key
0   -rwx   69040    Jun    17 2001 10:43:04   log_error_crashdump
0   -rwx   891      Apr    08 2000 11:14:28   sslt_key1.pem
0   -rwx   887      Jul    23 2001 17:24:00   ssh_host_rsa_key
0   -rwx   668      Jul    23 2001 17:24:34   ssh_host_dsa_key
0   -rwx   156      Apr    26 2001 13:57:46   dh512.pem
0   -rwx   245      Apr    26 2001 13:57:46   dh1024.pem
0   -rwx   0        May    09 2002 16:45:30   slog0.txt
```

show sysinfo

Данная команда предоставляет системную информацию о коммутаторе.

Формат show sysinfo

Режим Privileged EXEC

Термин	Значение
Switch Description	Текст, идентифицирующий данный коммутатор.
System Name	Имя, используемое для идентификации коммутатора. По умолчанию - пустое имя. Для настройки System Name см. "snmp-server".
System Location	Текст, описывающий местонахождение этого коммутатора. По умолчанию - пустой текст. Для настройки System Location см. "snmp-server".
System Contact	Текст, используемый для определения контактного лица. По умолчанию - пустой текст. Для настройки System Location см. "snmp-server".
System ObjectID	Базовый object ID для MIB коммутатора.
System Up Time	Время в днях, часах и минутах, прошедшее с последней перезагрузки коммутатора.
Current SNTP Synchronized Time	Системное время, полученное от сервера SNTP.

Термин	Значение
MIBs Supported	Список MIB, поддерживаемых данным агентом.

show tech-support

Данная команда отображает системную и конфигурационную информацию, которая требуется при общении с сотрудниками поддержки. Информация, возвращаемая командой show tech-support , состоит из вывода нескольких команд и включает в себя файлы журнала предыдущих запусков:

- show version
- show sysinfo
- show port all
- show logging
- show event log
- show logging buffered
- show msg-queue
- show trap log
- show running-config

Формат show tech-support

Режим Privileged EXEC

length value

Используйте эту команду, чтобы установить длину разбивки на страницы (количество строк) для сеансов, указанных при настройке в разных режимах Line Config (telnet / ssh / console). Команда действует постоянно.

ПРИМЕР: Команда Length в режиме Line Console применяется для подключения через консольный порт.

По умолчанию 24

Формат length *value*

Режим Line Config

no length value

Данная команда сбрасывает длину страницы на заводские значения.

Формат no length value

Режим Line Config

terminal length

Используйте эту команду, чтобы задать длину разбивки на страницы для текущего сеанса. Команда вступает в силу немедленно, и работает только для текущей сессии.

По умолчанию 24 строки на странице

Формат terminal length *value*

Mode Privileged EXEC

no terminal length

Используйте эту команду для сброса длины страницы на значения, настроенные в режиме Line Config в зависимости от типа сеанса.

Формат no terminal length *value*

Режим Privileged EXEC

show terminal length

Используйте эту команду для отображения всех настроенных значений длины страниц терминала.

Формат show terminal length

Режим Privileged EXEC

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show terminal length
Terminal Length:
----------------------
For Current Session.....24
For Serial Console .....24
For Telnet Sessions.....24
For SSH Sessions.....24
```

memory free low-watermark processor

Используйте эту команду для получения уведомлений в тех случаях, когда свободная память процессора падает ниже установленного порога. Уведомление генерируется, когда свободная память опускается ниже порогового значения. Другое уведомление генерируется после того как доступная память поднимается до значения в 10 процентов выше указанного порога. Чтобы предотвратить генерацию избыточных уведомлений, когда свободная память процессора колеблется вокруг настроенного порога, генерируется только одно уведомление о верхнем или нижнем пороге памяти в течение 60 секунд. Значения порогов указываются в КБ (килобайтах). Пороговое значение использования ЦП сохраняется после перезагрузки коммутатора.

Формат memory free low-watermark processor *1-1034956*

Режим Global Config

Параметр	Описание
low-watermark	Когда свободная память процессора падает ниже этого порога, запускается уведомление. Диапазон составляет от 1 до максимальной доступной памяти на коммутаторе. Значение по умолчанию - 0 (отключено).

6.5. Команды журналирования

В этом разделе описаны команды, используемые для настройки и просмотра журнала системы.

logging buffered

Эта команда включает журналирование.

По умолчанию отключено, critical при включении

Формат logging buffered

Режим Global Config

no logging buffered

Эта команда отключает буферное журналирование.

Формат no logging buffered

Режим Global Config

logging buffered wrap

Данная команда разрешает перезаписывание файла журнала. В противном случае логирование прекратится тогда, когда файл журнала достигает предельного объема.

По умолчанию включено

Формат logging buffered wrap

Режим Privileged EXEC

no logging buffered wrap

Данная команда запрещает перезаписывание журнала (таким образом, логирование прекращается по достижении предельного объема файла журнала).

Формат no logging buffered wrap

Режим Privileged EXEC

logging cli-command

Эта команда включает функцию ведения журнала команд CLI. Журнал позволяет коммутатору регистрировать все команды CLI, запущенные в системе. Команды хранятся в постоянном журнале. Команда **show logging persistent** отображает сохраненную историю команд.

По умолчанию включено

Формат logging cli-command

Режим Global Config

no logging cli-command

Данная команда отключает журналирование CLI.

Формат no logging cli-command

Режим Global Config

logging console

Эта команда включает журналирование в консоль. Вы можете указать значение уровня критичности *severitylevel* (целое число от 0 до 7), либо использовать одно из следующих ключевых слов: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), **or debug** (7).

По умолчанию отключено, critical (2) при включении

Формат logging console *[severitylevel]*

Режим Global Config

no logging console

Эта команда отключает журналирование в консоль.

Формат no logging console

Режим Global Config

logging host

Данная команда настраивает параметры удаленного журнала. Можно настроить до 8 хостов.

По умолчанию порт—514

уровень—critical (2)

Формат logging host {hostaddress|hostname} addresstype {port severitylevel}

Mode Global Config

Параметр	Описание
hostaddress| hostname	IP-адрес хоста.
address-type	Указывает тип адреса, ipv4, ipv6 или dns.
port	Номер порта, от 1 до 65535.

Параметр	Описание
severitylevel	Уровень критичности. Укажите это значение в виде целого числа от 0 до 7, или в виде одного из следующих ключевых слов: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), **or debug** (7).

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)# logging host google.com dns 214
(Routing) (Config)# logging host 10.130.64.88 ipv4 214 6
(Routing) (Config)# logging host 2000::150 ipv6 214 7
```

logging host reconfigure

Эта команда включает перенастройку хоста удаленного журнала.

Формат logging host reconfigure *hostindex*

Режим Global Config

Параметр	Описание
hostindex	Введите индекс хоста ведения журнала, для которого необходимо изменить IP-адрес.

logging host remove

Эта команда отключает удаленное журналирование на хост. См. “show logging hosts” для получения списка индексов хостов.

Формат logging host remove *hostindex*

Режим Global Config

logging syslog

Данная команда включает системный журнал.

Формат logging syslog

Режим Global Config

no logging syslog

Данная команда отключает системный журнал.

Формат no logging syslog

Режим Global Config

logging syslog port

Данная команда включает системный журнал. Параметр *portid* - целое число в диапазоне 1 – 65535.

По умолчанию отключено

Формат logging syslog port *portid*

Режим Global Config

no logging syslog port

Данная команда отключает системный журнал.

Формат no logging syslog port

Режим Global Config

logging syslog source-interface

Эта команда настраивает адрес-источник syslog (IP-адрес источника) для конфигурации сервера syslog. Выбранный IP-адрес интерфейса-источника используется для заполнения IP-заголовка пакетов протокола управления. Это позволяет устройствам безопасности (межсетевым экранам) определять пакеты, исходящие от конкретного коммутатора. Если интерфейс-источник не указан, первичный IP-адрес исходящего интерфейса используется в качестве адреса источника.

Формат logging syslog source-interface {*unit/slot/port* |{vlan *vlanid*}}

Режим Global Config

Параметр	Описание
unit/slot/port	Интерфейс маршрутизироемый на основе порта.
vlan-id	Настраивает интерфейс VLAN для использования в качестве IP-адреса источника. Диапазон VLAN ID - от 1 до 4093.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(config)#logging syslog source-interface loopback 0
(config)#logging syslog source-interface tunnel 0
(config)#logging syslog source-interface 0/4/1 (config)#logging syslog source-interface 1/0/1
```

no logging syslog source-interface

Данная команда отключает системный журнал.

Формат no logging syslog

Режим Global Config

show logging

Данная команда предоставляет информацию о настройках журналирования.

Формат show logging

Режим Privileged EXEC

Термин	Значение
Logging Client Local Port	Порт на приемнике/ретрансляторе, на который отправляются сообщения syslog.
Logging Client Source Interface	Показывает настроенный интерфейс-источник syslog (IP-адрес источника).
CLI Command Logging	Показывает, включено ли ведение журнала команд CLI.
Console Logging	Показывает, включено ли ведение журнала консоли.
Console Logging Severity Filter	Минимальная степень критичности для записи в консольный журнал. Сообщения с равным или превышающим уровнем критичности записываются.
Buffered Logging	Показывает, включено ли буферное журналирование.
Persistent Logging	Показывает, включено ли постоянное журналирование.
Persistent Logging Severity Filter	Минимальный уровень критичности, при котором записи журнала хранятся после перезагрузки системы.
Syslog Logging	Показывает, включено ли ведение журнала syslog.
Log Messages Received	Количество сообщений, полученных в процессе журналирования. Включает отброшенные и проигнорированные сообщения.
Log Messages Dropped	Количество сообщений, которые не были обработаны ввиду ошибки или нехватки ресурсов.
Log Messages Relayed	Количество сообщений, отправленных на приемник/ретранслятор.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show logging
```

Logging Client Local Port	514
Logging Client Source Interface	(not configured)
CLI Command Logging	disabled
Console Logging	enabled
Console Logging Severity Filter	error
Buffered Logging	enabled
Persistent Logging	disabled
Persistent Logging Severity Filter	alert
Syslog Logging	disabled
Log Messages Received	1010
Log Messages Dropped	0
Log Messages Relayed	0

show logging buffered

Данная команда отображает буферное журналирование (журналы системной загрузки и системной работы).

Формат show logging buffered

Режим Privileged EXEC

Термин	Значение
Buffered (In-Memory) Logging	Показывает, включено ли буферное журналирование.
Buffered Logging Wrapping Behavior	Показывает выбранный вариант поведения системы при превышении файлом журнала максимально допустимого объема.
Buffered Log Count	Счетчик действительных сообщений в журнале (буферном).

show logging hosts

Данная команда отображает все настроенные журналирующие хосты. Используйте символ “|” для отображения опций фильтрации вывода.

Формат show logging hosts

Режим Privileged EXEC

Термин	Значение
Host Index	(Используется для удаления хостов).

Термин	Значение
IP Address / Hostname	IP-адрес или имя хоста удаленного журнала.
Severity Level	Минимальная степень критичности для записи на указанный адрес. Возможные степени критичности: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).
Port	Номер порта сервера на локальном хосте, с которого отправляются сообщения syslog.
Host Status	Поле Status предоставляет текущее состояние статуса строки snmp. (Active, Not in Service, Not Ready).

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show logging hosts ?
<cr>    Press enter to execute the command. |
        Output filter options.

(Routing) #show logging hosts
Index   IP Address/Hostname     Severity    Port    Status
-----------------------------------------------------------------------------
1       10.130.64.88            critical    514     Active
2       2000::150               critical    514     Active
```

show logging persistent

Данная команда показывает записи постоянного журнала. С ключевым словом log-files - выводятся файлы постоянного системного журнала.

Формат show logging persistent [log-files]

Режим Privileged EXEC

Параметр	Описание
Persistent Logging	Показывает, включено ли постоянное журналирование.
Persistent Log Count	Счетчик сообщений в постоянном журнале.
Persistent Log Files	Список файлов постоянного системного журанла. Отображается только в том случае, если указано **log-files**.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Switching) #show logging persistent
Persistent Logging    : disabled
Persistent Log Count : 0
(Switching) #show logging persistent log-files
Persistent Log Files:
slog0.txt
slog1.txt slog2.txt olog0.txt olog1.txt olog2.txt
```

show logging traplogs

Данная команда отображает события и статистику SNMP trap.

Формат show logging traplogs

Режим Privileged EXEC

Термин	Значение
Number of Traps Since Last Reset	Количество SNMP trap со времени последней загрузки.
Trap Log Capacity	Количество trap, которое может поддерживать система.
Number of Traps Since Log Last Viewed	Количество новых trap с момента последнего запуска команды.
Log	Номер журнала.
System Time Up	Время непрерывной работы системы во время отправки SNMP trap.
Trap	Текст сообщения SNMP trap.

clear logging buffered

Данная команда очищает буферные журналы (журналы системной загрузки и системной работы).

Формат clear logging buffered

Режим Privileged EXEC

6.6. Команды почтового сервера и уведомлений по Email

logging email

Эта команда включает оповещение по электронной почте и устанавливает самый низкий уровень критичности отправки сообщений журнала. Если вы явно укажете уровень критичности, сообщения журнала этого уровня и выше, но ниже уровня urgent (см. далее)

будут отправлены по электронной почте по расписанию, собранные вместе к моменту истечения времени ожидания журнала. Вы можете указать значение уровня критичности **severitylevel** (целое число от 0 до 7), либо использовать одно из следующих ключевых слов: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).

По умолчанию отключено; при включении по почте отправляются сообщения критичности Warning (4) и выше.

Формат logging email *[severitylevel]*

Режим Global Config

no logging email

Данная команда отключает email-оповещение.

Формат no logging email

Режим Global Config

logging email urgent

Данная команда устанавливает низший уровень критичности, на котором сообщения журнала отправляются по почте немедленно (отдельным сообщением). Вы можете указать значение критичности **severitylevel** (целое число от 0 до 7), либо использовать одно из следующих ключевых слов: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), **or debug** (7). **none** – все сообщения журнала будут отправляться по временному интервалу (а не немедленно).

По умолчанию Сообщения критичности Alert (1) и Emergency (0) отправляются немедленно.

Формат logging email urgent {*severitylevel* | none}

Режим Global Config

no logging email urgent

Данная команда возвращает функции настройки по умолчанию.

Формат no logging email urgent

Режим Global Config

logging email message-type to-addr

Данная команда настраивает email-адреса, на которые отправляются сообщения. Поддерживаемые типы сообщений: **urgent** (срочные), **non-urgent** (несрочные), и **both** (оба типа). Для каждого поддерживаемого уровня критичности можно настроить несколько адресов. Переменная **to-email-addr** – это стандартный адрес email, например, admin@yourcompany.com.

Формат logging email message-type {urgent |non-urgent |both} to-addr *to-email-addr*

Режим Global Config

no logging email message-type to-addr

Данная команда удаляет настроенное поле «to-addr».

Формат no logging email message-type {urgent |non-urgent |both} to-addr *to-email-addr*

Режим Global Config

logging email from-addr

Эта команда настраивает адрес электронной почты отправителя (коммутатора).

По умолчанию switch@switch.com

Формат logging email from-addr *from-email-addr*

Режим Global Config

no logging email from-addr

Данная команда удаляет настроенный адрес отправителя.

Формат no logging email from-addr *from-email-addr*

Режим Global Config

logging email message-type subject

Данная команда настраивает тему письма для определенного типа сообщений.

По умолчанию Для срочных («urgent») сообщений: Urgent Log Messages

Для несрочных сообщений: Non Urgent Log Messages

Формат logging email message-type {urgent |non-urgent |both} subject *subject*

Режим Global Config

no logging email message-type subject

Данная команда возвращает настройки темы письма на значения по умолчанию, для определенного типа сообщений.

Формат no logging email message-type {urgent |non-urgent |both} subject

Режим Global Config

logging email logtime

Данная команда настраивает частоту отправки несрочных сообщений. Несрочные сообщения собираются и отправляются одним письмом по расписанию. Возможный диапазон значений: 30 – 1440 (в минутах).

По умолчанию 30 минут

Формат logging email logtime *minutes*

Режим Global Config

no logging email logtime

Данная команда возвращает настройки по умолчанию для временного интервала отправки несрочных сообщений.

Формат no logging email logtime

Режим Global Config

logging traps

Данная команда настраивает уровень критичности, при котором SNMP trap заносятся в журнал и отправляются по email. Вы можете указать значение критичности *severitylevel* (целое число от 0 до 7), либо использовать одно из следующих ключевых слов: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), **or debug** (7).

По умолчанию Сообщения Info (6) и выше заносятся в журнал.

Формат logging traps *severitylevel*

Режим Global Config

no logging traps

Данная команда возвращает функции настройки по умолчанию.

Формат no logging traps

Режим Global Config

logging email test message-type

Данная команда отправляет на SMTP-сервер письмо для тестирования функции оповещений по email.

Формат logging email test message-type {urgent |non-urgent |both} message-body *message-body*

Режим Global Config

show logging email config

Данная команда выводит на экран информацию о настройке функции оповещений по email.

Формат show logging email config

Режим Privileged EXEC

Термин	Значение
Email Alert Logging	Состояние функции: включена или выключена.
Email Alert From Address	Адрес электронной почты отправителя (коммутатора).
Email Alert Urgent Severity Level	Низший уровень критичности из тех, которые считаются срочными («urgent»). Срочные сообщения отправляются немеделенно.

Термин	Значение
Email Alert Non Urgent Severity Level	Низший уровень критичности, который считается несрочным. Несрочные сообщений собираются и отправляются одним письмом по расписанию. Сообщения журнала с еще более низким уровнем критичности (ниже несрочного) не отправляются по электронной почте вообще.
Email Alert Trap Severity Level	Низший уровень критичности, на котором trap заносятся в журнал.
Email Alert Notification Period	Временной интервал между отправками несрочных сообщений.
Email Alert To Address Table	Настроенные адреса получателей оповещений.
Email Alert Subject Table	Строки темы письма, включенные в сообщения срочные (Тип 1) и несрочные (Тип 2).
For Msg Type urgent, subject is	Настроенная тема письма для срочных сообщений.
For Msg Type non-urgent, subject is	Настроенная тема письма для несрочных сообщений.

show logging email statistics

Данная команда отображает статистику email-оповещений.

Формат show logging email statistics

Режим Privileged EXEC

Термин	Значение
Email Alert Operation Status	Состояние функции: включена или выключена.
No of Email Failures	Количество email-сообщений, попытка отправки которых не увенчалась успехом.
No of Email Sent	Количество сообщений, отправленных коммутатором с момента последнего сброса этого счетчика.

Термин	Значение
Time Since Last Email Sent	Время, прошедшее с момента отправки последнего сообщения.

clear logging email statistics

Данная команда сбрасывает статистику email-оповещений.

Формат clear logging email statistics

Режим Privileged EXEC

mail-server

Эта команда настраивает SMTP-сервер, на который коммутатор отправляет сообщения электронной почты и активирует режим Mail Server Configuration. Адрес сервера может быть в формате IPv4, IPv6 или DNS.

Формат mail-server {ip-address | ipv6-address | hostname}

Режим Config

no mail-server

Данная команда удаляет указанный сервер SMTP из конфигурации.

Формат no mail-server {ip-address | ipv6-address | hostname}

Режим Global Config

security

Эта команда устанавливает протокол безопасности уведомлений по электронной почте, позволяя коммутатору использовать аутентификацию TLS с SMTP-сервером. Если режим TLS включен на коммутаторе, но SMTP-сервер не поддерживает режим TLS, электронные письма на SMTP-сервер не отправляются.

По умолчанию нет

Формат security {tlsv1 | none}

Режим Mail Server Config

port

Эта команда настраивает TCP-порт, используемый для связи с SMTP-сервером. Рекомендуемый порт для TLSv1 – 465, а для незащищенного соединения (т.е. none) - 25. Тем не менее, разрешен любой нестандартный порт в диапазоне от 1 до 65535.

По умолчанию 25

Формат port {465 | 25 | 1–65535}

Режим Mail Server Config

username (Mail Server Config)

Эта команда настраивает имя пользователя, используемое для аутентификации на SMTP-сервере.

По умолчанию admin

Формат username *name*

Режим Mail Server Config

password

Эта команда настраивает пароль, используемый для аутентификации на SMTP-сервере.

По умолчанию admin

Формат password *password*

Режим Mail Server Config

show mail-server config

Данная команда выводит на экран информацию о настройке функции оповещений по email.

Формат show mail-server {*ip-address* | *hostname* | all} config

Режим Privileged EXEC

Термин	Значение
No of mail servers configured	Количество серверов SMTP, настроенных на коммутаторе.
Email Alert Mail Server Address	IPv4/IPv6-адрес или DNS-имя хоста настроенного сервера SMTP.
Email Alert Mail Server Port	TCP-порт, используемый коммутатором для отправки писем на сервер SMTP.
Email Alert Security Protocol	Протокол безопасности, используемый для аутентификации на SMTP-сервере (доступны TLS и работа без протокола безопасности).
Email Alert Username	Имя пользователя, используемое коммутатором для аутентификации на SMTP-сервере.
Email Alert Password	Пароль, используемый коммутатором для аутентификации на SMTP-сервере.

6.7. Команды системных утилит и команды Clear

В этом разделе описываются команды, которые используются, чтобы помочь устранить проблемы с подключением и восстановить различные конфигурации по умолчанию.

traceroute

Используйте команду traceroute для обнаружения маршрута следования пакетов IPv4 или IPv6 по принципу «шаг за шагом». Traceroute продолжает обеспечивать синхронный ответ, когда он инициируется из CLI.

Пользователь может указать исходный IP-адрес проверки traceroute. Обратите внимание, что принцип работы traceroute заключается в отправке пакетов, которые, как ожидается, не достигнут своего конечного адресата, а вместо этого запустят сообщения об ошибках ICMP обратно на исходный адрес, и так с каждого перехода по прямому пути к адресу назначения. Указав адрес источника, пользователь может определить, где по прямому пути нет обратного маршрута к исходному адресу. Обратите внимание, что это полезно только в том случае, если маршрут от источника к точке назначения и обратный маршрут от точки назначения к источнику являются симметричными. Распространенной практикой является, например, отправить трассировку с граничного маршрутизатора на целевую станцию выше в сети, используя адрес источника из подсети хоста на граничном маршрутизаторе. Это позволит проверить доступность маршрута внутри сети обратно на хосты, подключенные к граничному маршрутизатору. Также можно отправить traceroute с адресом интерфейса loopback в качестве источника для проверки доступности маршрута до адреса интерфейса loopback.

Пользователь может указать источник в виде адреса IPv4, IPv6-адрес или интерфейс маршрутизации. Когда источник указан как интерфейс маршрутизации, трассировка отправляется с использованием первичного адреса IPv4 на интерфейсе источника. С SNMP источник должен быть указан в виде адреса. Источник не может быть указан в Веб-интерфейсе.

Коммутатор не примет входящий пакет, в том числе ответ traceroute, если этот пакет поступает на интерфейс маршрутизации, а адрес назначения пакета находится на одном из интерфейсов управления вне диапазона (служебный порт или сетевой порт). Аналогично, коммутатор не примет пакет, который поступает на интерфейс управления, если адрес назначения пакета является адресом на интерфейсе маршрутизации. Таким образом, не имеет смысла отправлять трассировку на интерфейс управления с использованием адреса интерфейса маршрутизации в качестве источника, или же отправлять трассировку на интерфейс маршрутизации с использованием в качестве источника интерфейс управления. При отправке трассировки на интерфейс маршрутизации источником должен быть этот или другой интерфейс маршрутизации. При отправке трассировки на интерфейс управления источник должен находиться на этом интерфейсе управления. По этой причине пользователь не может указать источником интерфейс управления или адрес интерфейса управления. При отправке трассировки на интерфейс управления пользователь не должен указывать адрес источника, а вместо этого позволить системе выбирать адрес источника из исходящего интерфейса.

По умолчанию

- count: 3 попытки
- interval: 3 секунды
- size: 0 байт.
- port: 33434
- maxTtl: 30 переходов
- maxFail: 5 попыток
- initTtl: 1 переход

Формат traceroute {*ip-address* | [ipv6] {*ipv6-address* | *hostname*}} [initTtl *initTtl*] [maxTtl *maxTtl*] [maxFail *maxFail*] [interval *interval*] [count *count*] [port *port*] [size *size*] [source {*ip-address* | | *ipv6-address* | *unit/slot/port*}]

Режим Privileged EXEC

Используя параметры, описанные ниже, вы можете указать начальное и максимальное время жизни (TTL) в пробных пакетах, максимальное количество отказов до завершения, количество проверок отправленных для каждого TTL, и размер каждого пробного пакета.

Параметр	Описание
ipaddress	Действительный IP-адрес.
ipv6-address	Действительный адрес IPv6.
hostname	Действительное имя хоста.
ipv6	Необязательное ключевое слово «ipv6» может использоваться перед адресом IPv6 либо перед именем хоста. Во втором случае это вызовет попытку преобразовать имя хоста в адрес IPv6.
initTtl	**initTtl** определяет начальное TTL, то есть максимальное количество переходов на пути между локальной и удаленной системами. Диапазон - от 0 до 255.
maxTtl	**maxTtl** определяет максимальное TTL. Диапазон - от 1 до 255.
maxFail	**maxFail** останавливает процесс traceroute после определенного количества последовательных неудачных попыток получить ответ. Диапазон - от 0 до 255.
interval	Необязательный параметр **interval** определяет время между попытками, в секундах. Если ответ не получен за указанный временной интервал, утилита считает данную попытку неудачной (возвращая *) и совершает следующую. Если traceroute не получает ответа за указанный временной интервал, следующая попытка совершается немедленно. Диапазон - от 1 до 60 секунд.
count	Необязательный параметр **count** указывает количество попыток для каждого значения TTL. Диапазон - от 1 до 10 попыток.
port	Необязательный параметр **port** указывает порт назначения UDP. Этот порт на устройстве назначения должен быть свободным. Диапазон - от 1 до 65535.
size	Необязательный параметр **size** указывает объем полезной нагрузки эхо-запросов, в байтах. Диапазон - от 0 до 65507 байт.

Параметр	Описание
source	Необязательный параметр **source** указывает IP-адрес источника для traceroute.

Ниже приведен пример команды.

ПРИМЕР: Успешная трассировка:

(Routing) # traceroute 10.240.10.115 initTtl 1 maxTtl 4 maxFail 0 interval 1 count 3 port 33434 size 43

Traceroute to 10.240.10.115 ,4 hops max 43 byte packets:

1 10.240.4.1 708 msec 41 msec 11 msec

2 10.240.10.115 0 msec 0 msec 0 msec

Hop Count = 1 Last TTL = 2 Test attempt = 6 Test Success = 6

ПРИМЕР: Успешная трассировка IPv6:

(Routing) # traceroute 2001::2 initTtl 1 maxTtl 4 maxFail 0 interval 1 count 3

port 33434 size 43

Traceroute to 2001::2 hops max 43 byte packets:

1 2001::2 708 msec 41 msec 11 msec

Вышеприведенная команда также может выполняться с необязательным параметром «ipv6»:

(Routing) # traceroute ipv6 2001::2 initTtl 1 maxTtl 4 maxFail 0 interval 1 count 3

port 33434 size 43

ПРИМЕР: Ошибка traceroute:

(Routing) # traceroute 10.40.1.1 initTtl 1 maxFail 0 interval 1 count 3

port 33434 size 43

Traceroute to 10.40.1.1 ,30 hops max 43 byte packets:

1 10.240.4.1 19 msec 18 msec 9 msec

2 10.240.1.252 0 msec 0 msec 1 msec

3 172.31.0.9 277 msec 276 msec 277 msec

4 10.254.1.1 289 msec 327 msec 282 msec

5 10.254.21.2 287 msec 293 msec 296 msec

6 192.168.76.2 290 msec 291 msec 289 msec

7 0.0.0.0 0 msec *

Hop Count = 6 Last TTL = 7 Test attempt = 19 Test Success = 18

ПРИМЕР: Ошибка traceroute IPv6:

(Routing)# traceroute 2001::2 initTtl 1 maxFail 0 interval 1 count 3

port 33434 size 43

Traceroute to 2001::2 hops max 43 byte packets:

1 3001::1 708 msec 41 msec 11 msec

2 4001::2 250 msec 200 msec 193 msec

3 5001::3 289 msec 313 msec 278 msec

4 6001::4 651 msec 41 msec 270 msec

5 0 0 msec *

Hop Count = 4 Last TTL = 5 Test attempt = 1 Test Success = 0

clear config

Данная команда сбрасывает конфигурацию на заводские значения без отключения питания коммутатора. После запуска команды система запросит подтверждение. Введя y, вы сбрасываете конфигурацию коммутатора на настройки по умолчанию. Перезагрузки коммутатора при этом не происходит.

Формат clear config

Режим Privileged EXEC

clear counters

Данная команда очищает статистику указанных **unit/slot/port**, для всех портов либо для указанного интерфейса VLAN.

Формат clear counters {*unit/slot/port* | all | vlan *id*}

Режим Privileged EXEC

clear igmpsnooping

Эта команда очищает таблицы, управляемые функцией IGMP Snooping, и предпринимает попытку удалить эти записи из базы данных Multicast Forwarding (переадресации многоадресной передачи).

Формат clear igmpsnooping

Режим Privileged EXEC

clear pass

Данная команда сбрасывает все пользовательские пароли на значения по умолчанию без отключения питания коммутатора. После запуска команды система запросит подтверждение.

Формат clear pass

Режим Privileged EXEC

clear traplog

Данная команда очищает журнал trap.

Формат clear traplog

Режим Privileged EXEC

clear vlan

Данная команда сбрасывает конфигурацию VLAN на значения по умолчанию. Когда конфигурация VLAN сбрасывается до заводских значений по умолчанию, это вызывает некоторые сценарии, связанные с GVRP:

1. Удаляются статические VLAN.
2. В результате обработки события VEST RESTORE NOTIFY, GVRP восстанавливается до значения по умолчанию. GVRP по умолчанию деактивирован. Это означает, что GVRP должен быть отключен, и все его динамические VLAN должны быть удалены.

Формат clear vlan

Режим Privileged EXEC

logout

Эта команда закрывает текущее соединение telnet или сбрасывает текущее последовательное соединение.

ПРИМЕЧАНИЕ: Сохраните изменения конфигурации перед выходом.

Format logout

Режимы Privileged EXEC
User EXEC

ping

Данная команда позволяет определить доступность другого компьютера в сети. Пинг инициируется из командной строки либо Веб-интерфейса, и предполагает синхронный ответ.

ПРИМЕЧАНИЕ: Информация о команде **ping** для хостов IPv6 доступна по команде “ping ipv6”.

По умолчанию count: 1
interval: 3 (секунды)
size: 0 (байт).

Формат ping {*address*| *hostname* | {ipv6 {interface network *link-local-address* | *ipv6address* | *hostname*}} [count *count*] [interval 1-60] [size *size*] [source *ip-address* | *ipv6-address* | {*unit/slot/port* | vlan *1-4093* | network}]

Режимы Privileged EXEC
User EXEC

Используя настройки, описанные ниже, вы можете определить количество и размер пакетов эхо-запросов, а также интервал между ними.

Параметр	Описание
address	Адреса IPv4 или IPv6 для отправки эхо-запросов.
count	Количество пакетов ping, которые необходимо послать на адрес назначения (определяемый полем **ip-address**). Диапазон значений - от 1 до 15 запросов.

Параметр	Описание
interval	Время между попытками, в секундах. Диапазон - от 1 до 60 секунд.
size	Объем полезной нагрузки эхо-запросов, в байтах. Диапазон - от 0 до 65507 байт.
source	Адрес интерфейса-источника, используемый при отправке эхо-запросов.
hostname	Имя хоста для преобразования в адрес IPv4 или IPv6. Ключевое слово «ipv6» указывается, если требуется преобразовать адрес именно в IPv6. В противном случае будет использован адрес IPv4,
ipv6	Необязательное ключевое слово «ipv6» может использоваться перед адресом IPv6 либо перед именем хоста. Используйте опциональное ключевое слово «ipv6» перед именем хоста, чтобы попытаться преобразовать его в адрес IPv6 напрямую. Также используется для вызова локального IPv6-адреса.
interface	Ключевое слово, используемое для пинга локального адреса IPv6 через интерфейс.
link-localaddress	Локальный адрес IPv6 для пинга через интерфейс.

Ниже приведен пример команды.

ПРИМЕР: Успешный пинг IPv4:

```
(Routing) #ping 10.254.2.160 count 3 interval 1 size 255 Pinging 10.254.2.160 with 255 bytes of data:
Received response for icmp_seq = 0. time = 275268 usec
Received response for icmp_seq = 1. time = 274009 usec
Received response for icmp_seq = 2. time = 279459 usec
----10.254.2.160 PING statistics----
packets transmitted, 3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 274/279/276
```

ПРИМЕР: Успешный пинг IPv6:

```
(Routing) #ping 2001::1
Pinging 2001::1 with 64 bytes of data:
Send count=3, Receive count=3 from 2001::1 Average round trip time = 3.00 ms
```

ПРИМЕР: Неудачный пинг IPv4:

В случае недоступного адреса назначения:

(Routing) # ping 192.168.254.222 count 3 interval 1 size 255

Pinging 192.168.254.222 with 255 bytes of data:

Received Response: Unreachable Destination

Received Response :Unreachable Destination

Received Response :Unreachable Destination

----192.168.254.222 PING statistics----

3 packets transmitted,3 packets received, 0% packet loss round-trip (msec) min/avg/max = 0/0/0

В случае таймаута запроса:

(Routing) # ping 1.1.1.1 count 1 interval 3 Pinging 1.1.1.1 with 0 bytes of data:

----1.1.1.1 PING statistics----

1 packets transmitted,0 packets received, 100% packet loss round-trip (msec) min/avg/max = 0/0/0

ПРИМЕР: неуспешный пинг IPv6

(Routing) #ping ipv6 2001::4

Pinging 2001::4 with 64 bytes of data:

Send count=3, Receive count=0 from 2001::4 Average round trip time = 0.00 ms

quit

Эта команда закрывает текущее соединение telnet или сбрасывает текущее последовательное соединение. Перед выходом система предложит вам сохранить изменения в настройках.

Формат quit

Режимы Privileged EXEC

User EXEC

reload

Данная команда перезагружает коммутатор без отключения питания. Перезагрузкой в данном случае считается разрыв всех сетевых соединений и исполнение загрузочного кода. Для инициализации используется хранимая в коммутаторе конфигурация. После запуска команды система запросит подтверждение. На успешную перезагрузку указывают светодиодные индикаторы.

Формат reload [configuration [*scriptname*]]

Режим Privileged EXEC

Параметр	Описание
configuration	Корректно перезагружает конфигурацию. Если конфигурационный файл не указан - используется загрузочный файл конфигурации.

Параметр	Описание
scriptname	Файл конфигурации для загрузки. Имя файла должно быть указано с расширением.

copy

Данная команда загружает файлы на коммутатор и выгружает с коммутатора. Также команда может использоваться для управления образами (резервным и активным) в системе dual image. Загрузка и выгрузка файлов с сервера, с использованием FTP, TFTP, Xmodem, Ymodem либо Zmodem. При использовании протокола FTP требуется ввод пароля.

Формат copy source destination {verify | noverify}

Режим Privileged EXEC

Замените параметры *source* и *destination* значениями из Таблицы на странице 198. Вместо параметра *url* (назначения или источника), используйте следующие значения:

{xmodem | tftp://ipaddr|hostname | ip6address|hostname/filepath/filename [noval] | ftp://user@ipaddress | hostname/filepath/filename}

Параметр **verify | noverify** Доступен только если включена функция проверки образа/конфигурации. (см “file verify”). verify указывает, что для указанного загруженного изображения или файла конфигурации будет выполнена проверка цифровой подписи. noverify , соответственно, указывает, что такая проверка выполняться не будет.

Ключевое слово **ias-users** включает поддержку загрузки файлов пользовательских баз данных IAS. Когда загружается пользовательский файл IAS, пользовательская база данных IAS на коммутаторе заменяется на загруженную, вместе с пользователями и атрибутами. В команде **copy url ias-users**, для URL-адреса файла пользователей IAS используется одно из следующих::

{ { tftp://<ipaddr | hostname> | <ipv6address | hostname> /<filepath>/<filename> } | { sftp | scp://

<username>@<ipaddress>/<filepath>/<filename>} }

Для FTP, TFTP, SFTP и SCP параметр **ipaddr | hostname** - это IP-адрес или имя хоста сервера.

ПРИМЕЧАНИЕ: Максимальная длина пути файла – 160 символов, максимальная длина имени файла – 31 символ.

filepath – путь к файлу, который нужно загрузить или выгрузить, а *filename* – имя этого файла.

ПРИМЕЧАНИЕ: **ip6address** – это также действительный параметр для пакетов маршрутизации, поддерживающих IPv6.

ВНИМАНИЕ: НЕ ЗАБУДЬТЕ ВЫГРУЗИТЬ СУЩЕСТВУЮЩИЙ ФАЙЛ SWITCH.CFG С КОММУТАТОРА ПЕРЕД ЗАГРУЗКОЙ НОВОГО ОБРАЗА, ЧТОБЫ СДЕЛАТЬ РЕЗЕРВНУЮ КОПИЮ.

Источник	Назначение	Описание
nvram:application : *sourcefilename*	*url*	Имя файла исходного приложения.

Источник	Назначение	Описание
nvram:backup-config	nvram:startup-config	Копирует резервную конфигурацию в загрузочную.
nvram:clibanner	*url*	Копирует баннер командной строки на сервер.
nvram:cpupktcapture.pcap	*url*	Загружает файлы захвата пакетов ЦП.
nvram:crash-log	*url*	Копирует аварийный журнал на сервер.
nvram:errorlog	*url*	Копирует журнал ошибок на сервер.
nvram:factory-defaults	*url*	Выгружает файлы заводских настроек.
nvram:log	*url*	Копирует файл журнала на сервер.
nvram:operational-log	*url*	Копирует файл рабочего журнала на сервер.
nvram:script *scriptname*	*url*	Копирует укзанный конфигурационный скрипт на сервер.
nvram:startup-config	nvram:backup-config	Копирует загрузочную конфигурацию в резервную.
nvram:startup-config	*url*	Копирует загрузочную конфигурацию на сервер.
nvram:startup-log	*url*	Выгружает файл журнала загрузки.
nvram: tech-support	[unit *url unit id*]	Выгружает системную информацию и конфигурацию для технической поддержки.
nvram:traplog	*url*	Копирует файл журнала trap на сервер.
system:running-config	nvram:startup-config	Сохраняет запущенную конфигурацию в NVRAM.
system:running-config	nvram:factory-defaults	Сохраняет запущенную конфигурацию в NVRAM, в файл factory-defaults.
url	nvram:application *destfilename*	Имя файла назначения для файла приложения.

Источник	Назначение	Описание
url	nvram:clibanner	Загружает баннер командной строки в систему.
url	nvram:publickey-config	Загружает публичный ключ для проверки конфигурационного скрипта.
url	nvram:publickey-image	Загружает публичный ключ для проверки образа.
url	nvram:script *destfilename*	Загружает в систему файл конфигурационного скрипта. Во время загрузки команда проверяет скрипт. В случае какой-либо ошибки команда перечисляет все строки в конце процесса проверки и запрашивает подтверждение перед копированием файла скрипта.
url	nvram:script destfilename noval	При использовании данной опции команда «copy» не проверяет загруженный файл скрипта. Ниже приведен пример.
(Routing) #copy tftp://1.1.1.1/file.scr nvram:script file.scr noval		
url	nvram:sshkey-dsa	Загружает файл ключа SSH. Для получения дополнительной информации см. раздел "Команды Secure Shell51".
url	nvram:sshkey-rsa1	Загружает файл ключа SSH.
url	nvram:sshkey-rsa2	Загружает файл ключа SSH.
url	nvram:sslpem-dhweak	Загружает сертификат HTTP secure-server.
url	nvram:sslpem-dhstrong	Загружает сертификат HTTP secure-server.
url	nvram:sslpem-root	Загружает сертификат HTTP secure-server. Для получения дополнительной информации см. раздел "Команды HTTP".
url	nvram:sslpem-server	Загружает сертификат HTTP secure-server.

Источник	Назначение	Описание
url	nvram:startup-config	Загружает в систему загрузочный конфигурационный файл.
url	ias-users	Загружает в систему файл базы данных пользователей IAS. Когда загружается пользовательский файл IAS, база данных пользователей IAS на коммутаторе заменяется на загруженную, вместе с пользователями и их атрибутами.
url	nvram:tech-supportcmds	Загружает файл, содержащий список команд, которые отображаются при выполнении команды show tech-support.
url	{active | backup}	Загружает образ с удаленного сервера (в качестве любого из двух образов).
{active | backup}	url	Выгружает активный или резервный образ на удаленный сервер.
active	backup	Заменяет резервный образ копией активного образа.
backup	active	Заменяет активный образ копией резервного образа.

ПРИМЕР: Ниже иллюстрируется загрузка и применение базы данных пользователей IAS.

```
(Routing) #copy tftp://10.131.17.104/aaa_users.txt ias-users
Mode ..... TFTP
Set Server IP ..... 10.131.17.104
Path ..... ./
Filename ..... aaa_users.txt Data
Type ..... IAS Users

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
File transfer operation completed successfully.
Validating and updating the users to the IAS users database.
Updated IAS users database successfully.
(Routing) #
```

file verify

Эта команда позволяет выполнять проверку цифровой подписи при загрузке образа и/или файла конфигурации на коммутатор.

Формат file verify {all | image | none | script}

Режим Global Config

Параметр	Описание
All	Проверяет цифровую подпись файлов и образа, и конфигурации.
Image	Проверяет цифровую подпись файлов образа.
None	Не проверяет цифровую подпись ни у образа, ни у конфигурации.
Script	Проверяет цифровую подпись файлов конфигурации.

no file verify

Сбрасывает настройки проверки цифровой подписи на заводские значения.

Формат no file verify

Режим Global Config

write memory

Используйте эту команду, чтобы сохранить текущие изменения конфигурации в NVRAM, чтобы изменения, которые вы вносите, сохранялись при перезагрузке. Команда работает так же, как команда **copy system:running-config nvram:startup-config**. Используйте ключевое слово **confirm**, чтобы напрямую сохранить конфигурацию в NVRAM без запроса подтверждения.

Формат write memory [confirm]

Режим Privileged EXEC

6.8. Команды Power over Ethernet

В этом разделе описываются команды, используемые для настройки и мониторинга Power Over Ethernet (PoE). PoE позволяет IP-телефонам, точкам доступа Wi-Fi и другим устройствам получать питание и данные по существующим кабелям локальной сети без изменения существующей инфраструктуры Ethernet. PoE поддерживается только на коммутаторах, имеющих контроллер PoE.

PoE реализует спецификацию PoE+ (IEEE 802.3at) для оборудования источника питания (PSE). IEEE 802.3at позволяет подавать питание на питаемые устройства (PD) 4 класса, для которых требуется мощность от 15,4 до 34,2 Вт. Это позволяет использовать сетевые коммутаторы и маршрутизаторы с поддержкой PoE+ для развертывания с устройствами, которым требуется больше мощности, чем позволяет спецификация 802.3AF. PoE+ 802.3at совместим с 802.1AF.

Гибкое управление мощностью

PoE обеспечивает управление питанием, с поддержкой резервирования, приоритизацию и ограничение мощности. Оператор может назначить приоритет каждому порту PoE. Когда бюджет мощности коммутатора PoE исчерпывается, более приоритетным портам отдается предпочтение по сравнению с портами с более низким приоритетом. Подача мощности на порты с более низким приоритетом принудительно прекращается, чтобы обеспечить питание портов с более высоким приоритетом.

Статическая функция управления питанием позволяет операторам резервировать гарантированную мощность для порта PoE. Это полезно для питания устройств, которые потребляют переменное количество энергии и обеспечивают им гарантированный диапазон мощности для работы. Помимо пользовательского управления мощностью, поддерживается функция распределения мощности на основе класса.

В функции динамического управления мощностью питание не резервируется для какого-либо порта в определенный момент времени. Мощность, доступная с помощью PoE-коммутатора, рассчитывается путем вычитания мгновенной мощности, потребляемой всеми портами, из максимальной доступной мощности. Таким образом, одновременно возможно обеспечить питанием большее количество портов Эта функция полезна для эффективного питания большего количества устройств в тех случаях, когда доступная мощность на PoE-коммутаторе ограничена.

PoE также предоставляет глобальную функцию порога использования, чтобы ограничить коммутатор PoE от перегрузки. Оператор может указать лимит в процентах от максимальной мощности.

ПРИМЕЧАНИЕ: Команды PoE применимы только к медным портам.

poe high-power

Используйте эту команду для включения режима высокой мощности для определенного коммутатора (режим Interface Configuration). В режиме высокой мощности коммутатор согласовывает бюджет мощности с питаемым устройством (PD, powered device). Максимальная мощность, которую может обеспечить PoE-порт, составляет 32 Вт в режиме dot3at и 60 Вт в режиме upoe.

По умолчанию Отключено

Формат poe high-power {dot3at | legacy | pre-dot3at}

Режим Interface Configuration

Параметр	Описание
dot3at	Устройства высокой мощности с поддержкой LLDP.
legacy	Устройства с высоким пусковым током.
pre-dot3at	Устройства без поддержки LLDP.

no poe high-power

Отключает режим высокой мощности.

Формат no poe high-power

Режим Interface Configuration

poe power limit

Используйте эту команду для настройки ограничения мощности для всех портов на всех коммутаторах (режим Global Configuration) или на определенном порте (режим Interface Configuration).

По умолчанию Пользовательское значение

Формат poe power limit . {dot3af | none | userd-defined [3000-30000]}

Режим Global Configuration

Interface Configuration

Параметр	Описание
none	Нет лимита мощности.
userd-defined	Ограничение мощности заданное пользователем. Диапазон 3000-60000 мВт на порт.

no power power limit

Данная команда сбрасывает настройки лимита мощности на заводские значения.

По умолчанию Пользовательское значение

Формат no poe power limit

Режим Global Configuration

Interface Configuration

poe power management

Данная команда настраивает тип управления подачей питания.

По умолчанию Dynamic

Формат poe power management {*unit/slot/port* | all} {dynamic | static}

Режим Global Configuration

Параметр	Описание
unit	Настраивает управление питанием для отдельного порта.
Параметр	Описание
all	Настраивает управление питанием для всех портов.
dynamic	Управление питанием осуществляется PoE-контроллером, максимальная мощность для порта не резервируется.
static	Управление питанием осуществляется PoE-контроллером, максимальная мощность для порта резервируется.

no poe power management

Данная команда сбрасывает настройки режима управления на заводские значения.

Формат no poe power management

Режим Global Configuration

poe priority

Используйте эту команду для настройки уровня приоритета порта для подачи питания на подключенное устройство. Коммутатор может не справиться с обеспечением питания всех подключенных устройств, поэтому приоритет порта используется для определения того, какие порты будут обеспечены питанием в случае нехватки общей мощности. Для портов с одинаковым уровнем приоритета порт с более низким номером имеет более высокий приоритет.

Если система уже обеспечивает максимально возможную мощность, и при этом к порту с более высоким приоритетом подключается новое устройство - подача питания на порт с более низким приоритетом прекращается в пользу более приоритетного порта.

По умолчанию Low (низкий)

Формат poe priority { Crit | High | Medium | Low }

Режим Global Configuration

Interface Configuration

no poe priority

Данная команда сбрасывает настройки приоритета порта (или портов) на значения по умолчанию.

По умолчанию Low (низкий)

Формат no poe priority

Режим Global Configuration

Interface Configuration

poe reset

Данная команда сбрасывает все порты.

По умолчанию Отключено

Формат poe reset

Режим Global Configuration
Interface Configuration

poe traps

Используйте эту команду для включения / выключения отправки trap, которые указывают на изменения статуса PoE для порта.

По умолчанию включено

Формат poe traps

Режим Global Configuration

poe usagethreshold

Используйте эту команду для настройки порогового уровня использования мощности системы, при котором создается trap. Порог настраивается как процент от общей доступной мощности.

По умолчанию 90%

Формат poe usagethreshold {unit | all} *1-99*

Режим Global Configuration

Параметр	Описание
unit	Устанавливает пороговое значения для коммутатора.
all	Устанавливает пороговое значения для всех коммутаторов.
1-99	Пороговое значение мощности, при котором генерируется trap. Диапазон: 1 – 99%.

no poe usagethreshold

Данная команда сбрасывает порог на заводские значения.

Формат no poe usagethreshold

Режим Global Configuration

show poe

Данная команда отображает текущую конфигурацию PoE и информацию о состоянии для всех портов.

Формат show poe

Режим Privileged EXEC

ПРИМЕР:

```
(Switching) #show poe
Firmware Version                1.3.0.7
PSE Main Operational Status     OFF
Threshold Power                 459000 mW
Total Power Consumed            0
Usage Threshold                 90
Power Management Mode           Dynamic
Traps                           Enable
```

show poe port configuration

Используйте эту команду для отображения информации о конфигурации порта PoE для отдельного порта либо для всех портов.

Формат show poe ports configuration {all | unit/slot/port}

Режим Privileged EXEC

ПРИМЕР:

(Switching) #show poe port configuration 0/1

Intf	Admin Mode	Priority	Power Limit (mW)	Power Limit Type	High Power Mode	Detection Type	Timer Schedule
0/1	Enable	Low	60000	User Defined	UPOE	auto	None

show poe port info

Данная команда отображает информацию о PoE портах.

Формат show poe port info { all | *unit/slot/port* }

Режим Privileged EXEC

ПРИМЕР:

(Switching) #show poe port info all

Intf	High Power	Max Power (mW)	Class	Power (mW)	Output Current (mA)	Output Voltage (V)	Status	Fault Status
2/0/1	Yes	32000	Unknown	0	0	0	Disabled	No Error
2/0/2	Yes	32000	Unknown	0	0	0	Disabled	No Error
2/0/3	Yes	32000	Unknown	0	0	0	Disabled	No Error
2/0/4	Yes	32000	Unknown	0	0	0	Disabled	No Error
2/0/5	Yes	32000	Unknown	0	0	0	Disabled	No Error
2/0/6	Yes	32000	Unknown	0	0	0	Disabled	No Error
2/0/7	Yes	32000	Unknown	0	0	0	Disabled	No Error
2/0/8	Yes	32000	Unknown	0	0	0	Disabled	No Error
2/0/9	Yes	32000	Unknown	0	0	0	Disabled	No Error
2/0/10	Yes	32000	Unknown	0	0	0	Disabled	No Error
2/0/11	Yes	32000	Unknown	0	0	0	Disabled	No Error
2/0/12	Yes	32000	Unknown	0	0	0	Disabled	No Error
2/0/13	Yes	32000	Unknown	0	0	0	Disabled	No Error
2/0/14	Yes	32000	Unknown	0	0	0	Disabled	No Error
2/0/15	Yes	32000	Unknown	0	0	0	Disabled	No Error

2/0/16	Yes	32000	Unknown	0	0	0	Disabled	No Error
2/0/17	Yes	32000	Unknown	0	0	0	Disabled	No Error
2/0/18	Yes	32000	Unknown	0	0	0	Disabled	No Error

6.9. Команды SNTP

В этом разделе описаны команды, используемые для автоматической настройки времени и даты системы при помощи протокола SNTP (Simple Network Time Protocol).

sntp broadcast client poll-interval

Эта команда устанавливает интервал опроса для клиентов широковещательной передачи SNTP в секундах, где pollinterval может быть значением от 6 до 10.

По умолчанию 6

Формат sntp broadcast client poll-interval *poll-interval*

Режим Global Config

no sntp broadcast client poll-interval

Данная команда возвращает заводские значения интервала опроса.

Формат no sntp broadcast client poll-interval

Режим Global Config

sntp client mode

Данная команда активирует клиентский режим протокола SNTP, и также может включить одноадресный либо широковещательный режим.

По умолчанию отключено

Формат sntp client mode [*broadcast* | *unicast*]

Режим Global Config

no sntp client mode

Данная команда отключает клиентский режим SNTP.

Формат no sntp client mode

Режим Global Config

sntp client port

Эта команда устанавливает ID порта клиента SNTP равным 0, 123, либо значению между 1025 и 65535. Значение по умолчанию равно 0, что означает, что порт SNTP не настроен пользователем. В этом случае фактическое значение порта клиента, используемое в SNTP-пакетах, назначается базовой ОС.

По умолчанию 0

Формат sntp client port portid

Режим Global Config

no sntp client port

Данная команда возвращает настройки клиентского порта SNTP на значения по умолчанию.

Формат no sntp client port

Режим Global Config

sntp unicast client poll-interval

Эта команда устанавливает интервал опроса для клиентов одноадресной передачи SNTP в секундах, где- interval может быть значением от 6 до 10.

По умолчанию 6

Формат sntp unicast client poll-interval poll-interval

Режим Global Config

no sntp unicast client poll-interval

Данная команда возвращает заводские значения интервала опроса.

Формат no sntp unicast client poll-interval

Режим Global Config

sntp unicast client poll-timeout

Эта команда устанавливает тайм-аут опроса для одноадресных клиентов SNTP в секундах, в диапазоне от 1 до 30.

По умолчанию 5

Формат sntp unicast client poll-timeout poll-timeout

Режим Global Config

no sntp unicast client poll-timeout

Данная команда возвращает настройки таймаута опроса для оодноадресных клиентов SNTP на заводские значения.

Формат no sntp unicast client poll-timeout

Режим Global Config

sntp unicast client poll-retry

Эта команда настраивает количество повторов опроса для одноадресных клиентов протокола SNTP, в диапазоне от 0 до 10.

По умолчанию 1

Формат sntp unicast client poll-retry *poll-retry*

Режим Global Config

no sntp unicast client poll-retry

Данная команда возвращает настройки количества повторов опроса для одноадресных клиентов протокола SNTP на заводские значения.

Формат no sntp unicast client poll-retry

Режим Global Config

sntp server

Данная команда настраивает SNTP-сервер (до 3 серверов). Адрес сервера может быть как IPv4, так и IPv6. Диапазоны возможных значений: приоритет - от 1 до 3, версия - от 1 до 4, ID порта - от 1 до 65535.

Формат sntp server {ipaddress | ipv6address | hostname} [priority [version [portid]]]

Режим Global Config

no sntp server

Данная команда удаляет сервер из списка настроенных серверов SNTP.

Формат no sntp server remove {*ipaddress* | *ipv6address* | *hostname*}

Режим Global Config

sntp source-interface

Используйте эту команду, чтобы указать физический или логический интерфейс для использования в качестве исходного интерфейса (IP-адреса источника) для конфигурации одноадресного сервера SNTP. Если адрес исходного интерфейса настроен, он используется для всех SNTP-коммуникаций между сервером и клиентом. Выбранный IP-адрес интерфейса-источника используется для заполнения IP-заголовка пакетов протокола управления. Это позволяет устройствам безопасности (межсетевым экранам) определять пакеты, исходящие от конкретного коммутатора. Если интерфейс-источник не указан, первичный IP-адрес исходящего интерфейса используется в качестве исходного адреса. Если сконфигурированный интерфейс не работает, клиент SNTP возвращается к его поведению по умолчанию.

Формат sntp source-interface {*unit/slot/port* | vlan *vlan-id*}

Режим Global Config

Параметр	Описание
unit/slot/port	Идентификатор, назначенный коммутатору.
vlan-id	Настраивает интерфейс VLAN для использования с IP-адресом источника. Диапазон VLAN ID - от 1 до 4093.

no sntp source-interface

Данная команда используется для сброса интерфейса-источника SNTP на настройки по умолчанию.

Формат no sntp source-interface

Режим Global Config

show sntp

Данная команда используется для отображения настроек и состояния SNTP.

Формат show sntp

Режим Privileged EXEC

Термин	Значение
Last Update Time	Время последней синхронизации системных часов.
Last Attempt Time	Время последнего запроса на передачу (в одноадресном режиме).
Last Attempt Status	Статус последнего SNTP-запроса (в одноадресном режиме) или незапрошенного сообщения (в режиме широковещания).
Broadcast Count	Текущее количество незапрошенных широковещательных сообщений, которые были получены и обработаны клиентом SNTP с момента последней перезагрузки.

show sntp client

Данная команда используется для отображения настроек SNTP-клиента.

Формат show sntp client

Режим Privileged EXEC

Термин	Значение
Client Supported Modes	Поддерживаемые режимы SNTP (одноадресные и широковещательные).
SNTP Version	Наивысшая версия SNTP, поддерживаемая клиентом.
Port	Порт SNTP-клиента. 0 означает значение по умолчанию. Когда значение порта клиента равно 0, клиент в режиме широковещательной передачи привязывается к порту 123; клиент же в одноадресном режиме привязывается к порту, назначенному базовой ОС.

Термин	Значение
Client Mode	Настроенный режим SNTP-клиента.

show sntp server

Данная команда используется для отображения настроек SNTP-сервера и списка настроенных серверов.

Формат show sntp server

Режим Privileged EXEC

Термин	Значение
Server Host Address	IP-адрес или имя хоста настроенного сервера SNTP.
Server Type	Тип адреса сервера (IPv4, IPv6, или DNS).
Server Stratum	Заявленный уровень стратум сервера для последнего принятого действительного пакета.
Server Reference ID	Идентификатор системных часов сервера для последнего принятого действительного пакета.
Server Mode	Режим сервера SNTP.
Server Maximum Entries	Общее допустимое количество серверов SNTP.
Термин	Значение
Server Current Entries	Общее количество настроенных SNTP.

Для каждого сконфигурированного сервера:

Термин	Значение
IP Address / Hostname	IP-адрес или имя хоста настроенного сервера SNTP.
Address Type	Тип адреса сервера (IPv4, IPv6, или DNS).
Priority	Тип IP-приоритета настроенного сервера.
Version	Версия протокола SNTP на сервере. Версия протокола используется для запросов к серверу в одноадресном режиме.

Термин	Значение
Port	Номер порта сервера.
Last Attempt Time	Время последней попытки для указанного сервера.
Last Update Status	Состояние последней попытки для сервера.
Total Unicast Requests	Количество запросов на сервер.
Failed Unicast Requests	Количество неудачных запросов от сервера.

show sntp source-interface

Данная команда используется для отображения интерфейса-источника SNTP-клиента, настроенного на коммутаторе.

Формат show sntp source-interface

Режим Privileged EXEC

Поле	Описание
SNTP Client Source Interface	Идентификатор интерфейса физического или логического, настроенного в качестве интерфейса-источника клиента SNTP.
SNTP Client Source IPv4 Address	IP-адрес интерфейса, настроенного в качестве интерфейса-источника клиента SNTP.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show sntp source-interface
SNTP Client Source Interface..... (not configured)
(Routing) #
```

6.10. Команды часового пояса

Эти команды позволяют настроить системные дату и время, часовой пояс и переход на летнее время. Переход на летнее время может быть повторяющимся либо единократным.

clock set

Эта команда устанавливает системные время и дату.

Формат clock set *hh:mm:ss*

clock set *mm/dd/yyyy*

Режим Global Config

Параметр	Описание
hh:mm:ss	Введите текущее время в 24-часовом формате: часы, минуты и секунды. Возможные диапазоны: часы от 0 до 23, минуты: от 0 до 59, секунды: от 0 до 59.
mm/dd/yyyy	Введите дату в следующем формате: месяц, день и год. Диапазон месяцев - от 1 до 12. Диапазон дней - от 1 до 31. Диапазон годов - от 2010 до 2079.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)# clock set 03:17:00
(Routing) (Config)# clock set 11/01/2011
```

clock summer-time date

Используйте команду «clock summer-time date» для установки перехода на летнее время. Если необязательные параметры не указаны, они принимаются как либо 0, либо \0, в зависимости от ситуации.

Формат clock summer-time date {date month year hh:mm date month year hh:mm}[offset offset] [zone acronym]

Режим Global Config

Параметр	Описание
date	День месяца. Диапазон - от 1 до 31.
month	Месяц. Введите первые три буквы названия месяца на английском языке (например, «jan»).
year	Год. Диапазон - от 2000 до 2097.
hh:mm	Время в 24-часовом формате в часах и минутах. Возможные диапазоны: часы от 0 до 23, минуты: от 0 до 59.
offset	Количество минут, которые необходимо добавить при переходе на летнее время. Диапазон - от 1 до 1440.
acronym	Сокращение для часового пояса, который используется коммутатором при переходе на летнее время. Допустимо до 4 символов.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)# clock summer-time date 1 nov 2011 3:18 2 nov 2011 3:18
```

(Routing) (Config)# clock summer-time date 1 nov 2011 3:18 2 nov 2011 3:18 offset 120 zone INDA

clock summer-time recurring

Эта команда устанавливает параметры повторющегося перехода на летнее время.

Формат clock summer-time recurring {week day month hh:mm week day month hh:mm} [offset offset] [zone acronym]

Режим Global Config

Параметр	Описание
EU	Система использует правила перехода на летнее время, принятые в Европейском Союзе.
USA	Система использует правила перехода на летнее время, принятые в США.
week	Неделя месяца. Диапазон - от 1 до 5, а также «first» (первая) и «last» (последняя).
day	День недели. Введите первые три буквы названия дня недели на английском языке (например, «sun»).
month	Месяц. Введите первые три буквы названия месяца на английском языке (например, «jan»).
hh:mm	Время в 24-часовом формате в часах и минутах. Возможные диапазоны: часы от 0 до 23, минуты: от 0 до 59.
offset	Количество минут, которые необходимо добавить при переходе на летнее время. Диапазон - от 1 до 1440.
acronym	Сокращение для часового пояса, который используется коммутатором при переходе на летнее время. Допустимо до 4 символов.

ПРИМЕР: Ниже приведен пример выполнения команды.

(Routing) (Config)# clock summer-time recurring 2 sun nov 3:18 2 mon nov 3:18

(Routing) (Config)# clock summer-time recurring 2 sun nov 3:18 2 mon nov 3:18 offset 120 zone INDA

no clock summer-time

Эта команда отключает переход на летнее время.

Формат no clock summer-time

Режим Global Config

ПРИМЕР: Ниже приведен пример выполнения команды.

(Routing) (Config)# no clock summer-time

clock timezone

Данная команда позволяет настроить часовой пояс UTC. Если необязательные параметры не указаны, они принимаются как либо **0**, либо **\0** в зависимости от ситуации.

Формат clock timezone {*hours*} [minutes *minutes*] [zone *acronym*]

Режим Global Config

Параметр	Описание
hours	Отклонение часового пояса от UTC. Диапазон - от -12 до +13.
minutes	Отклонение в минутах от времени UTC. Диапазон - от 0 до 59.
acronym	Сокращение, обозначающее часовой пояс. Допустимо до 4 символов.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)# clock timezone 5 minutes 30 zone INDA
```

no clock timezone

Данная команда используется для обнуления параметров часового пояса.

Формат no clock timezone

Режим Global Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)# no clock timezone
```

show clock

Данная команда отображает дату и время системных часов.

Формат show clock

Режим Privileged EXEC

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) # show clock
15:02:09 (UTC+0:00) Nov 1 2011
No time source
```

ПРИМЕР: Вывод командной строки для данной команды.

С приведенной выше конфигурацией вывод выглядит следующим образом:

```
(Routing) # show clock
10:55:40 INDA(UTC+7:30) Nov 1 2011
No time source
```

show clock detail

Используйте эту команду для отображения подробного системного времени вместе с часовым поясом и настройками перехода на летнее время.

Формат show clock detail

Режим Privileged EXEC

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) # show clock detail
15:05:24 (UTC+0:00) Nov 1 2011
No time source
Time zone:
Acronym not configured
Offset is UTC+0:00
Summertime:
Summer-time is disabled
```

ПРИМЕР: Вывод командной строки для данной команды.

С приведенной выше конфигурацией вывод выглядит следующим образом:

```
(Routing) # show clock detail
10:57:57 INDA(UTC+7:30) Nov 1 2011
No time source
Time zone:
Acronym is INDA
Offset is UTC+5:30
Summertime:
Acronym is INDA
Recurring every year
Begins on second Sunday of Nov at 03:18
Ends on second Monday of Nov at 03:18
Offset is 120 minutes
Summer-time is in effect.
```

6.11. Команды DHCP-сервера

В этом разделе описаны команды, который используется для настройки DHCP-сервера на коммутаторе. DHCP использует UDP в качестве транспортного протокола и поддерживает ряд функций, которые облегчают администрирование распределения адресов.

ip dhcp pool

Данная команда позволяет настроить пул адресов DHCP и активирует режим DHCP pool configuration.

По умолчанию нет

Формат ip dhcp pool name

Режим Global Config

no ip dhcp pool

Данная команда удаляет пул DHCP. «Name» - ранее настроенное название пула.

Формат no ip dhcp pool name

Режим Global Config

client-identifier

Эта команда позволяет указать уникальный идентификатор для DHCP-клиента. Уникальный идентификатор - это допустимая нотация в шестнадцатеричном формате. В некоторых системах (например клиенты Microsoft DHCP), идентификатор клиента требуется вместо аппаратного адреса. Уникальный идентификатор представляет собой сочетание типа среды передачи данных и MAC-адреса. Например, идентификатор клиента Microsoft для Ethernet-адреса c819.2488.f177 выглядит как 01c8.1924.88f1.77, где 01 говорит о типе среды передачи данных Ethernet. Для получения дополнительной информации о нумерации разных типов среды обратитесь к разделу "Address Resolution Protocol Parameters" RFC 1700.

По умолчанию нет

Формат client-identifier uniqueidentifier

Режим DHCP Pool Config

no client-identifier

Данная команда удаляет идентификатор клиента.

Формат no client-identifier

Режим DHCP Pool Config

client-name

Эта команда позволяет указать имя для DHCP-клиента. Имя - текстовая строка, состоящая из стандартных символов ASCII.

По умолчанию нет

Формат client-name name

Режим DHCP Pool Config

no client-name

Данная команда удаляет имя клиента.

Формат no client-name

Режим DHCP Pool Config

default-router

Эта команда позволяет указать список маршрутизаторов по умолчанию для DHCP-клиента. {address1, address2… address8} - действительные IP-адреса, состоящие из десятичных чисел от 0 до 255. IP-адрес 0.0.0.0 не является действительным.

По умолчанию нет

Формат default-router address1 [address2....address8]

Режим DHCP Pool Config

no default-router

Данная команда удаляет список маршрутизаторов по умолчанию.

Формат no default-router

Режим DHCP Pool Config

dns-server

Эта команда позволяет указать доступные для DHCP-клиента DNS-сервера. Параметр «address» - это действительные IP-адреса, состоящие из десятичных чисел от 0 до 255. IP-адрес 0.0.0.0 не является действительным.

По умолчанию нет

Формат dns-server address1 [address2....address8]

Режим DHCP Pool Config

no dns-server

Данная команда удаляет список DNS-серверов.

Формат no dns-server

Режим DHCP Pool Config

hardware-address

Эта команда позволяет указать аппаратный адрес DHCP-клиента. Аппаратный адрес - это MAC-адрес аппаратной платформы клиента, состоящий из 6 байтов в шестнадцатеричном формате с разделением точками. «Type» - протокол аппаратной платформы. Он равняется 1 для 10 МБ Ethernet, и 6 – для IEEE 802.

По умолчанию ethernet

Формат hardware-address *hardwareaddress type*

Режим DHCP Pool Config

no hardware-address

Данная команда удаляет аппаратный адрес DHCP-клиента.

Формат no hardware-address

Режим DHCP Pool Config

host

Данная команда указывает IP-адрес и маску подсети для привязки к клиенту DHCP вручную. Параметры «**address**» и «**mask**» - это действительные IP-адреса, состоящие из десятичных чисел от 0 до 255. IP-адрес 0.0.0.0 не является действительным. «**Prefix-length**» – целое число от 0 до 32.

По умолчанию нет

Формат host address [{mask | prefix-length}]

Режим DHCP Pool Config

no host

Данная команда удаляет IP-адреса DHCP-клиента.

Формат no host

Режим DHCP Pool Config

lease

Данная команда настраивает продолжительность аренды IP-адреса, выдаваемого клиенту сервером DHCP. Общее время аренды должно быть в пределах 1-86400 мин. *Infinite* – установить время аренды в 60 дней. Вы также можете настроить другое время аренды. *Days* (дни) – целое число от 0 до 59. *Hours* (часы) – целое число от 0 до 23. *Minutes* (минуты) – целое число от 0 до 59.

По умолчанию 1 день

Формат **lease [{days [hours] [minutes] | infinite}]**

Режим DHCP Pool Config

no lease

Данная команда сбрасывает время аренды DHCP на значения по умолчанию.

Формат no lease

Режим DHCP Pool Config

network (DHCP Pool Config)

Используйте эту команду для настройки адрес подсети и маски для пула адреса DHCP на сервере. «**networknumber**» – допустимый IP-адрес, состоящий из четырех десятичных чисел в диапазоне от 0 до 255. IP-адрес 0.0.0.0 не является действительным. «*mask*» – это маска подсети IP для указанного пула адресов. «**prefix-length**» – целое число от 0 до 32.

По умолчанию нет

Формат network networknumber [{mask | prefixlength}]

Режим DHCP Pool Config

no network

Данная команда удаляет адрес подсети и маску.

Формат no network

Режим DHCP Pool Config

bootfile

Эта команда позволяет указать имя загрузочного образа по умолчанию для DHCP-клиента. **filename** – файл загрузочного образа.

Формат bootfile *filename*

Режим DHCP Pool Config

no bootfile

Данная команда удаляет имя загрузочного образа.

Формат no bootfile

Режим DHCP Pool Config

domain-name

Эта команда позволяет указать доменное имя для DHCP-клиента. *domain* – доменное имя.

По умолчанию нет

Формат domain-name *domain*

Режим DHCP Pool Config

no domain-name

Данная команда удаляет доменное имя.

Формат no domain-name

Режим DHCP Pool Config

netbios-name-server

Эта команда настраивает серверы имен NetBIOS Windows Internet Naming Service (WINS), доступные для клиентов DHCP.

Требуется один IP-адрес, хотя в командной строке можно указать до восьми адресов за раз. Сервера указываются в порядке приоритета (address1 - самый предпочтительный сервер, address2 - следующий за ним по предпочтению, и т.д.).

По умолчанию нет

Формат netbios-name-server *address* [*address2...address8*]

Режим DHCP Pool Config

no netbios-name-server

Данная команда удаляет список серверов NetBIOS.

Формат no netbios-name-server

Режим DHCP Pool Config

netbios-node-type

Данная команда настраивает тип узла NetBIOS для Microsoft DHCP-клиентов. «Type» указывает тип узла NetBIOS. Допустимые типы:

- b-node—Широковещательный
- p-node—Одноранговый (peer-to-peer)
- m-node—Смешанный
- h-node—Гибридный (рекомендуется)

По умолчанию нет

Формат netbios-node-type *type*

Режим DHCP Pool Config

no netbios-node-type

Данная команда удаляет тип узла NetBIOS.

Формат no netbios-node-type

Режим DHCP Pool Config

next-server

Эта команда настраивает следующий сервер в процессе загрузки клиента DHCP. Параметр **address** – это IP-адрес следующего сервера (обычно это TFTP-сервер).

По умолчанию вспомогательные адреса входящего интерфейса

Формат next-server *address*

Режим DHCP Pool Config

no next-server

Данная команда удаляет список загрузочных серверов.

Формат no next-server

Режим DHCP Pool Config

option

Данная команда настраивает опции сервера DHCP. Параметр *code* указывает код опции DHCP и находится в диапазоне от 1 до 254. Параметр *ascii string* указывает строку символов NVT ASCII. Символьные строки ASCII, содержащие пробелы, должны быть заключены в кавычки. Параметр **hex string** указывает шестнадцатеричные данные. В шестнадцатеричной строке символьные строки представляют собой две шестнадцатеричные цифры. Вы можете разделить каждый байт точкой (например, a3.4f.22.0c), двоеточием (например, a3: 4f: 22: 0c) или пробелом (например, a3 4f 22 0c).

По умолчанию нет

Формат option code {ascii string | hex string1 [string2...string8] | ip address1 [address2...address8]}

Режим DHCP Pool Config

no option

Данная команда удаляет опции сервера DHCP. Параметр *code* указывает код опции DHCP.

Формат no option *code*

Режим DHCP Pool Config

ip dhcp excluded-address

Эта команда указывает IP-адреса, которые DHCP-сервер не должен назначать клиентам DHCP. Параметры «low-address» и «high-address» - это действительные IP-адреса, состоящие из десятичных чисел от 0 до 255. IP-адрес 0.0.0.0 не является дейсвительным.

По умолчанию нет

Формат ip dhcp excluded-address *lowaddress [highaddress]*

Режим Global Config

no ip dhcp excluded-address

Данная команда удаляет удаляет IP-адреса из списка адресов, которые сервер не должен назначать клиентам DHCP. Параметры «low-address» и «high-address» - это действительные IP-адреса, состоящие из десятичных чисел от 0 до 255. IP-адрес 0.0.0.0 не является действительным.

Формат no ip dhcp excluded-address *lowaddress [highaddress]*

Режим Global Config

ip dhcp ping packets

Используйте эту команду, чтобы указать количество пакетов (в диапазоне от 2 до 10), которые DHCP-сервер отправляет на адрес пула как часть операции ping. По умолчанию количество пакетов, отправленных в адрес пула, равно 2, что является наименьшим допустимым количеством. Установка количества пакетов на 0 отключает эту команду.

По умолчанию 2

Формат ip dhcp ping packets *0,2-10*

Режим Global Config

no ip dhcp ping packets

Данная команда возвращает заводские значения количества пакетов ping.

Формат no ip dhcp ping packets

Режим Global Config

service dhcp

Данная команда активирует DHCP-сервер.

По умолчанию отключено

Формат service dhcp

Режим Global Config

no service dhcp

Данная команда отключает DHCP-сервер.

Формат no service dhcp

Режим Global Config

ip dhcp bootp automatic

Эта команда позволяет назначить адреса клиенту bootp. Адреса берутся из автоматического пула адресов.

По умолчанию отключено

Формат ip dhcp bootp automatic

Режим Global Config

no ip dhcp bootp automatic

Эта команда отключает выдачу адресов клиенту bootp.

Формат no ip dhcp bootp automatic

Режим Global Config

ip dhcp conflict logging

Данная команда активирует ведение журнала о конфликтах на DHCP-сервере.

По умолчанию включено

Формат ip dhcp conflict logging

Режим Global Config

no ip dhcp conflict logging

Данная команда отключает ведение журнала о конфликтах на DHCP-сервере.

Формат no ip dhcp conflict logging

Режим Global Config

clear ip dhcp binding

Данная команда удаляет автоматическую привязку адресов из базы данных DHCP-сервера. Если указать “*”, удаляются привязки, соотетствующие всем адресам. address – допустимый IP-адрес, состоящий из четырех десятичных чисел в диапазоне от 0 до 255. IP-адрес 0.0.0.0 не является действительным.

Формат clear ip dhcp binding {*address* | *}

Режим Privileged EXEC

clear ip dhcp server statistics

Данная команда обнуляет счётчики статистики DHCP.

Формат clear ip dhcp server statistics

Режим Privileged EXEC

clear ip dhcp conflict

Данная команда удаляет конфликт адресов из базы данных DHCP-сервера. Сервер обнаруживает конфликты посредством пинга. DHCP-сервер очищает все конфликты, если к параметру «address» добавлен символ «*».

По умолчанию нет

Формат clear ip dhcp conflict {*address* | *}

Режим Privileged EXEC

show ip dhcp binding

Эта команда отображает привязки адресов для определенного IP-адреса на DHCP-сервере. Если IP-адрес не указан, отображаются привязки, соответствующие всем адресам.

Формат show ip dhcp binding [*address*]

Режимы Privileged EXEC

User EXEC

Термин	Значение
IP address	IP-адрес клиента.
Hardware Address	MAC-адрес или идентификатор клиента.
Lease expiration	Время истечения срока аренды выданного IP-адреса.
Type	Способ, которым IP-адрес был назначен клиенту.

show ip dhcp global configuration

Эта команда отображает глобальные настройки DHCP сервера.

Формат show ip dhcp global configuration

Режимы Privileged EXEC

User EXEC

Термин	Значение
Service DHCP	Поле, отображающее состояние протокола DHCP.
Number of Ping Packets	Максимальное количество пакетов Ping, которые будут отправляться, чтобы проверить, что IP-адрес еще не выдан.
Conflict Logging	Показывает, включено ли ведение журнала конфликтов.
BootP Automatic	Показывает, включен или отключен BootP для динамических пулов.

show ip dhcp pool configuration

Данная команда предоставляет информацию о настройках пула all – показать конфигурацию всех пулов.

Формат show ip dhcp pool configuration {*name* | all}

Режимы Privileged EXEC

User EXEC

Поле	Значение
Pool Name	Имя настроенного пула.
Pool Type	Тип пула.
Lease Time	Время истечения срока аренды выданного IP-адреса.
DNS Servers	Список DNS-серверов, доступных для клиента DHCP.
Default Routers	Список маршрутизаторов по умолчанию для DHCP-клиента.

Следующие поля - дополнительные, они отображаются для пулов типа Dynamic.

Поле	Значение
Network	Адрес сети и маска для пула адресов DHCP.

Следующие поля - дополнительные, они отображаются для пулов типа Manual.

Поле	Значение
Client Name	Имя клиента DHCP.
Client Identifier	Уникальный идентификатор клиента DHCP.
Hardware Address	Аппаратный адрес DHCP-клиента.

Поле	Значение
Hardware Address Type	Протокол аппаратной платформы.
Host	IP-адрес и маска подсети для привязки к клиенту DHCP вручную.

show ip dhcp server statistics

Данная команда отображает статистику DHCP-сервера.

Формат show ip dhcp global statistics

Режим Privileged EXEC

User EXEC

Поле	Значение
Automatic Bindings	Количество IP-адресов, автомаически привязанных к MAC-адресам хостов, которые находятся в базе данных DHCP.
Expired Bindings	Количество истекших сроков аренды.
Malformed Bindings	Количество неполных или поврежденных сообщений, полученных сервером DHCP.

Полученные сообщения:

Сообщение	Значение
DHCP DISCOVER	Количество сообщений DHCPDISCOVER, полученных сервером.
DHCP REQUEST	Количество сообщений DHCPREQUEST, полученных сервером.
DHCP DECLINE	Количество сообщений DHCPDECLINE, полученных сервером.
DHCP RELEASE	Количество сообщений DHCPRELEASE, полученных сервером.
DHCP INFORM	Количество сообщений DHCPINFORM, полученных сервером.

Отправленные сообщения:

Сообщение	Значение
DHCP OFFER	Количество сообщений DHCPOFFER, отправленных сервером.
DHCP ACK	Количество сообщений DHCPACK, отправленных сервером.
DHCP NACK	Количество сообщений DHCPNACK, отправленных сервером.

show ip dhcp conflict

Данная команда отображает записи о конфликтах адресов в журнале DHCP-сервера. Если IP-адрес не указан - отображаются записи обо всех конфликтах адресов.

Формат show ip dhcp conflict [*ip-address*]

Режим Privileged EXEC

User EXEC

Термин	Значение
IP address	IP-адрес хоста, согласно записи журнала DHCP-сервера.
Detection Method	Способ, которым на DHCP-сервере был обнаружен IP-адрес хоста.
Detection time	Время обнаружения конфликта.

6.12. Команды клиента DNS

Эти команды используются в DNS (Domain Name System). DNS позволяет преобразовывать доменные имена в IP-адреса. При включении клиент DNS предоставляет службу поиска хоста другим компонентам коммутатора.

ip domain lookup

Данная команда включает DNS-клиент.

По умолчанию включено

Формат ip domain lookup

Режим Global Config

no ip domain lookup

Данная команда отключает DNS-клиент.

Формат no ip domain lookup

Режим Global Config

ip domain name

Данная команда определяет доменное имя по умолчанию, используемое программным обеспечением коммутатора для завершения неполных имен хостов. Доменного имени по умолчанию нет. Параметр доменного имени *name* не может быть длиннее 255 символов и не может начинаться с точки. Параметр *name* следует использовать только в том случае пустого списка доменных имён (настраиваемого командой ip domain list).

По умолчанию нет

Формат ip domain name name

Режим Global Config

ПРИМЕР: Команда **ip domain name yahoo.com** устанавливает «yahoo.com» в качестве доменного имени по умолчанию. Для неполного имени «xxx» осуществляется DNS-запрос, который попытается найти IP-адрес, соответствующий «xxx.yahoo.com».

no ip domain name

Данная команда удаляет доменное имя по умолчанию, установленное командой **ip domain name**.

Формат no ip domain name

Режим Global Config

ip domain list

Данная команда позволяет создать список доменных имен по умолчанию для завершения неполных имен хостов. По умолчанию данный список пуст. Каждое доменное имя не может быть длиннее 256 символов и не может начинаться с точки. Доменное имя по умолчанию, созданное командой **ip domain name command**, используется только при пустом списке доменных имён. Список может содержать до 32 доменных имен.

По умолчанию нет

Формат ip domain list name

Режим Global Config

no ip domain list

Данная команда удаляет доменное имя из списка.

Формат no ip domain list *name*

Режим Global Config

ip name server

Данная команда настраивает доступные серверы имен. Можно настроить до 8 серверов, одной командой или в несколько приёмов. **server-address** – действительный IPv4 или IPv6 адрес сервера.

Выбор серверов определяется порядком из указания.

Формат ip name-server server-address1 [server-address2...server-address8]

Режим Global Config

no ip name server

Данная команда удаляет сервер имен.

Формат no ip name-server [server-address1...server-address8]

Режим Global Config

ip name source-interface

Используйте эту команду, чтобы указать физический или логический интерфейс для использования в качестве интерфейса-источника DNS-клиента (IP-адрес источника) для приложения управления DNS-клиентами. Если адрес интерфейса источника настроен, он используется для всех DNS-коммуникаций между сервером и клиентом. Выбранный IP-адрес интерфейса-источника используется для заполнения IP-заголовка пакетов протокола управления. Это позволяет устройствам безопасности (межсетевым экранам) определять пакеты, исходящие от конкретного коммутатора. Если интерфейс источника не указан, в качестве него используется первичный IP-адрес исходящего интерфейса. Если сконфигурированный интерфейс не работает, клиент DNS возвращается к его поведению по умолчанию.

Формат ip name source-interface {*unit/slot/port* | network | vlan *vlan-id*}

Режим Global Config

no ip name source-interface

Данная команда используется для сброса интерфейса-источника DNS на настройки по умолчанию.

Формат no ip name source-interface

Режим Global Config

ip host

Используйте эту команду для определения статического сопоставления имен и адресов в кэше хоста. Параметр **name** – имя хоста, **ip address** – IP-адрес хоста. Имя хоста может содержать 1 – 255 символов: букв, цифр, точек, дефисов, символов подчеркивания и пробелов (не идущих друг за другом). Если имя хоста содержит пробелы - его необходимо заключить в кавычки, например, “**lab-pc 45**”.

По умолчанию нет

Формат Ip host *name ipaddress*

Режим Global Config

no ip host

Данная команда удаляет сопоставление имен и адресов.

Формат no ip host *name*

Режим Global Config

ipv6 host

Используйте эту команду для определения статического сопоставления имен и адресов IPv6 в кэше хоста. Параметр **name** – имя хоста, **v6 address** – IPv6-адрес хоста. Имя хоста может содержать 1 – 255 символов: букв, цифр, точек, дефисов и пробелов. Если имя хоста содержит пробелы - его необходимо заключить в кавычки, например, “**lab-pc 45**”.

По умолчанию нет

Формат ipv6 host *name v6 address*

Режим Global Config

no ipv6 host

Используйте эту команду для удаления статического сопоставления имен и адресов IPv6 в кэше хоста.

Формат no ipv6 host *name*

Режим Global Config

ip domain retry

Используйте эту команду, чтобы указать количество попыток повторной отправки запросов DNS. Параметр **number** – количество попыток. Диапазон значений: 0 – 100.

По умолчанию 2

Формат ip domain retry number

Режим Global Config

no ip domain retry

Данная команда возвращает заводские значения.

Формат no ip domain retry number

Режим Global Config

ip domain timeout

Используйте эту команду, чтобы указать время ожидания перед повторной отправкой запроса DNS. Параметр **seconds** – время ожидания (в секундах). Диапазон значений: 0 – 3600.

По умолчанию 3

Формат ip domain timeout *seconds*

Режим Global Config

no ip domain timeout

Данная команда возвращает заводские значения.

Формат no ip domain timeout *seconds*

Режим Global Config

clear host

Используйте эту команду для удаления записей из кеша сопоставления имен и адресов хоста. Эта команда очищает записи из кэша DNS, поддерживаемые программным обеспечением. Команда очищает записи как IPv4, так и IPv6.

Формат clear host {*name* | all}

Режим Privileged EXEC

Поле	Описание
name	Имя хоста для удаления. Параметр *name* может иметь в длину 1 – 255 символов.
all	Удалить все записи.

show hosts

Данная команда отображает доменное имя по умолчанию, список серверов имен хостов, статический и кешированный список имен хостов и адресов. Параметр *name* может иметь в длину 1 – 255 символов. Команда показывает как записи IPv4, так и IPv6.

Формат show hosts *[name]*

Режим Privileged EXEC

User EXEC

Поле	Описание
Host Name	Доменное имя хоста.
Default Domain	Домеенное имя по умолчанию.
Default Domain List	Список доменов по умолчанию.
Domain Name Lookup	Состояние DNS-клиента: включен или выключен.
Number of Retries	Количество попыток повторной отправки запросов DNS.
Retry Timeout Period	Время ожидания перед повторной отправкой запроса DNS.
Name Servers	Настроенные сервера имён.
DNS Client Source Interface	Настроенный интерфейс-источник (IP-адрес источника), используемый клиентом DNS. IP-адрес выбранного интерфейса используется как адрес источника для всей коммуникации с сервером.

ПРИМЕР: Вывод командной строки для данной команды.

```
<Switching> show hosts
Host name      Device
Default domain                          gm.com
Default domain list                     yahoo.com, Stanford.edu, rediff.com
Domain Name lookup                      Enabled
Number of retries                       5
Retry timeout period                    1500
Name servers (Preference order)         176.16.1.18 176.16.1.19
DNS Client Source Interface             (not configured)

Configured host name-to-address mapping:
Host                        Addresses
--------------------------------------
accounting.gm.com           176.16.8.8

Host                 Total       Elapsed     Type        Addresses
-------------------------------------------------------------------
www.stanford.edu     72          3           IP          171.64.14.203
```

6.13. Команды конфликта IP-адресов

Команды данного раздела помогают устранять проблемы, связанные с конфликтом IP-адресов.

ip address-conflict-detect run

Данная команда запускает функцию активного обнаружения конфликтов IP-адресов коммутатора, путем рассылки ничем не вызванных ARP-пакетов на IPv4-адреса на коммутаторе.

Формат ip address-conflict-detect run

Режим Global Config0

show ip address-conflict

Эта команда отображает информацию о состоянии, соответствующую последнему обнаруженному конфликту адресов.

Формат show ip address-conflict

Режимы Privileged EXEC

Термин	Значение
Address Conflict Detection Status	Определяет, обнаружил ли коммутатор конфликт IP-адресов.
Last Conflicting IP Address	Последний IP-адрес, замеченный в ситуации конфликта на любом интерфейсе.
Last Conflicting MAC Address	MAC-адрес последнего обнауруженного конфликтующего хоста на любом интерфейсе.
Time Since Conflict Detected	Время в днях, часах, минутах и секундах с момента последнего обнаружения конфликта.

clear ip address-conflict-detect

Данная команда очищает информацию о конфликтах адресов.

Формат clear ip address-conflict-detect

Режим Privileged EXEC

6.14. Команды трассировки пакетов обслуживания

Данные команды позволяют сетевым администраторам диангостировать условия, влияющие на работу коммутатора.

ПРИМЕЧАНИЕ: Вывод команды “debug” может занять некоторое время и повлиять на производительность системы.

capture start

Данная команда вручную запускает процесс захвата пакетов ЦП для трассировки.

Процесс захвата происходит в трех режимах:

- Захват файла
- Удаленный захват
- Линейный захват

Действие этой команды прекращается при перезагрузке коммутатора.

Формат capture start [{all|receive|transmit}]

Режим Privileged EXEC

Параметр	Описание
all	Захват всего траффика.
receive	Захват только полученного трафиика.
transmit	Захат только передаваемого траффика.

capture stop

Данная команда останавливает процесс захвата пакетов ЦП для трассировки.

Формат capture stop

Режим Privileged EXEC

capture file|remote|line

Данная команда настраивает параметры захвата файлов. Перезагрузка не прекращает действие этой команды.

Формат capture {file|remote|line}

Режим Global Config

Параметр	Описание
file	В режиме захвата файла захваченные пакеты сохраняются в файл на NVRAM. Максимальный размер файла по умолчанию - 524288 байт. Коммутатор может передать файл на TFTP-сервер через TFTP, SFTP, SCP, CLI и SNMP. Файл отформатирован в формате pcap, имеет название cpuPktCapture.pcap и может быть проверен с использованием инструментов сетевого анализа, таких как Wireshark или Ethereal. Запуск захвата файлов автоматически прекращает любые сессии захвата и удаленные, и линейные. После активации захвата пакетов процедура продолжается до тех пор, пока файл захвата не достигнет своего максимального размера или пока захват не будет остановлен вручную с помощью команды capture stop.

Параметр	Описание
remote	В режиме удаленного захвата пакеты перенаправляются в реальном времени на внешний ПК, на котором запущен инструмент Wireshark для Microsoft Windows. Сервер захвата пакетов работает со стороны коммутатора и отправляет захваченные пакеты через TCP-соединение на Wireshark. Удаленный захват можно включить или отключить через интерфейс командной строки. Для отображения захваченного файла необходим ПК с Windows и установленной программой Wireshark. При использовании режима удаленного захвата коммутатор не сохраняет захваченные данные локально в своей файловой системе. Вы можете настроить номер порта IP для подключения Wireshark к коммутатору. Номер порта по умолчанию - 2002. Если между ПК Wireshark и коммутатором установлен межсетевой экран, порту должны быть разрешен доступ. Вы должны настроить сетевой экран, чтобы компьютер с Wireshark мог инициировать TCP-подключения к коммутатору. Если клиент успешно подключается к коммутатору, пакеты ЦП отправляются на клиентский ПК, затем Wireshark получает пакеты и отображает их. Это продолжается до тех пор, пока сеанс не будет завершен одной из сторон. Запуск сеанса удаленного захвата автоматически завершает захват файла и линейный захват.
line	В режиме линейного захвата захваченные пакеты сохраняются в ОЗУ и могут отображаться в CLI. Запуск линейного захвата автоматически завершает любой сеанс удаленного захвата и захвата в файл. В этом режиме могут быть захвачены до 128 пакетов размером до 128 байт.

capture remote port

Данная команда настраивает параметры удаленного захвата. Команда сохраняется после перезагрузки. Параметр *id* – номер порта TCP в диапазоне 1024 – 49151.

Формат capture remote port *id*

Режим Global Config

capture file size

Данная команда настраивает параметры захвата файлов. Команда сохраняется после перезагрузки. Параметр **maxfile-size** – максимальный размер, достижимый файлом pcap, в диапазоне 2 – 512 КБ.

Формат capture file size *max file size*

Режим Global Config

capture line wrap

Эта команда позволяет перезаписывать захваченные пакеты в режиме line, когда общий объем захваченных пакетов достигает предельной емкости.

Формат capture line wrap

Режим Global Config

no capture line wrap

Эта команда запрещает перезаписывать захваченные пакеты в режиме line, когда общий объем захваченных пакетов достигает предельной емкости.

Формат no capture line wrap

Режим Global Config

show capture packets

Используйте эту команду для отображения пакетов, захваченных и сохраненных в ОЗУ. Записывать и сохранять в ОЗУ можно те пакеты, которые принимаются или передаются через ЦП. За один сеанс захвата в ОЗУ может быть сохранено до 128 пакетов, размером до 128 байт. Если пакет содержит более 128 байт, сохраняются только первые 128; данные, превышающие 128 байт, пропускаются и не могут отображаться в CLI.

Захват пакетов прекращается автоматически после 128 пакетов, не отображенных во время сеанса захвата. Захваченные пакеты не сохраняются после перезагрузки.

Формат show capture packets

Режим Privileged EXEC

debug aaa accounting

Данная команда полезна для отладки конфигурации и функциональности учета в менеджере пользователей.

Формат debug aaa accounting

Режим Privileged EXEC

no debug aaa accounting

Данная команда отключает отладку функциональности учёта менеджера пользователей.

Формат no debug aaa accounting

Режим Privileged EXEC

debug arp

Данная команда включает отладочные сообщения протокола ARP.

По умолчанию отключено

Формат debug arp

Режим Privileged EXEC

no debug arp

Данная команда отключает отладочные сообщения протокола ARP.

Формат no debug arp

Режим Privileged EXEC

debug auto-voip

Данная команда включает отладочные сообщения Auto VOIP. Необязательные параметры позволяют отслеживать пакеты H323, SCCP или SIP.

По умолчанию отключено

Формат debug auto-voip [H323|SCCP|SIP]

Режим Privileged EXEC

no debug auto-voip

Данная команда отключает отладочные сообщения Auto VOIP.

Формат no debug auto-voip

Режим Privileged EXEC

debug clear

Данная команда отключает все ранее активированные отладочные трассировки.

По умолчанию отключено

Формат debug clear

Режим Privileged EXEC

debug console

Эта команда позволяет отображать вывод «отладочной» трассировки на авторизованной сессии, в которой она выполняется. Вывод отладки в консоль должен быть включен для просмотра любого вывода трассировки. Вывод команд отладочной трассировки будет отображаться во всех авторизованных сессий, для которых была включена консоль отладки. Конфигурация этой команды остается в силе до завершения сеанса входа в систему. Эффект данной команды не сохраняется после перезагрузки.

По умолчанию отключено

Формат debug console

Режим Privileged EXEC

no debug console

Эта команда отключает отображение вывода «отладочной» трассировки на авторизованной сессии, в которой она выполняется.

Формат no debug console

Режим Privileged EXEC

debug crashlog

Используйте эту команду для просмотра информации, содержащейся в файле журнала сбоев, который система поддерживает при непредвиденной перезагрузке. Файл журнала сбоев содержит следующую информацию:

- Информация вызова стека в формах primitive и verbose
- Состояние журнала
- Буферное журналирование
- Журнал событий
- Постоянное журналирование
- Системная информация (вывод sysapiMbufDump)
- Отладочная информация очереди сообщений
- Информация отладки памяти
- Состояние отладки памяти
- Информация о ОС (вывод osapiShowTasks)
- Информация /proc (meminfo, cpuinfo, interrupts, version и net/sockstat)

По умолчанию отключено

Формат debug crashlog {[kernel] *crashlog-number* [upload *url*] | proc | verbose | deleteall}

Режим Privileged EXEC

Параметр	Описание
kernel	Просмотр файла журнала сбоев ядра
crashlog-number	Указывает номер файла для просмотра. Система поддерживает до четырех копий, а допустимый диапазон 1 – 4.
upload url	Чтобы выгрузить журнал сбоев (или аварийный дамп) на TFTP-сервер, используйте ключевое слово upload и укажите необходимую информацию о TFTP-сервере.
proc	Просмотр журнала сбоев процесса приложения.
verbose	Активация подробного журнала сбоев.
deleteall	Удаляет все файлы журналов сбоев из системы.
data	Регистратор данных журнала сбоев.
crashdump-number	Указывает номер дампа сбоя для просмотра. Диапазон: 0 – 2.
download url	Чтобы загрузить аварийный дамп в коммутатор, используйте ключевое слово download и укажите необходимую информацию о TFTP-сервере.

Параметр	Описание
component-id	ID компонента, вызвавшего сбой.
item-number	Номер элемента.
additional-parameter	Дополнительные параметры.

debug debug-config

Используйте эту команду для загрузки или выгрузки файла debug-config.ini. Файл debug-config.ini выполняет команды CLI (включая команды devshell и drivshell) для определенных предварительно указанных событий. Отладочный конфигурационный файл создаётся вручную и загружается на коммутатор.

По умолчанию отключено

Формат debug debug-config {download <*url*> | upload <*url*>}

Режим Privileged EXEC

debug dhcp packet

Эта команда отображает отладочную информацию о действиях клиента DHCPv4 и трассировку пакетов DHCPv4 на локальный клиент DHCPv4 и обратно.

По умолчанию отключено

Формат debug dhcp packet [transmit | receive]

Режим Privileged EXEC

no debug dhcp

Эта команда отключает отображение вывода отладочной трассировки для активности клиента DHCPv4.

Формат no debug dhcp packet [transmit | receive]

Режим Privileged EXEC

debug dot1x packet

Используйте эту команду, чтобы включить отладочную трассировку пакетов dot1x.

По умолчанию отключено

Формат debug dot1x

Режим Privileged EXEC

no debug dot1x packet

Используйте эту команду, чтобы отключить отладочную трассировку пакетов dot1x.

Формат no debug dot1x

Режим Privileged EXEC

debug igmpsnooping packet

Эта команда позволяет отслеживать пакеты IGMP Snooping, полученные и переданные коммутатором.

По умолчанию отключено

Формат debug igmpsnooping packet

Режим Privileged EXEC

no debug igmpsnooping packet

Данная команда отключает отслеживание пакетов IGMP Snooping.

Формат no debug igmpsnooping packet

Режим Privileged EXEC

debug igmpsnooping packet transmit

Эта команда позволяет отслеживать пакеты IGMP Snooping, переданные коммутатором. Snooping должен быть включен на устройстве и интерфейсе для мониторинга пакетов для определенного интерфейса.

По умолчанию отключено

Формат debug igmpsnooping packet transmit

Режим Privileged EXEC

ПРИМЕР: вывода сообщения трассировки показан ниже.

<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]: igmp_snooping_debug.c(116) 908 % Pkt TX

- Intf: 1/0/20(20), Vlan_Id:1 Src_Mac: 00:03:0e:00:00:00 Dest_Mac: 01:00:5e:00:00:01 Src_IP: 9.1.1.1 Dest_IP: 225.0.0.1 Type: V2_Membership_Report Group: 225.0.0.1

В сообщении трассировки отображаются следующие параметры:

Параметр	Значение
TX	Пакет, переданный устройством.
Intf	Интерфейс, через который вышел пакет. Указывается в формате unit/slot/port (внутренний номер интерфейса). Значение «unit» для коммутаторов не в стеке всегда показывается как 1.
Src_Mac	MAC-адрес источника пакета.
Dest_Mac	Многоадресный MAC-адрес назначения пакета.
Src_IP	IP-адрес источника в заголовке пакета.

Параметр	Значение
Dest_IP	Многоадресный IP-адрес назначения пакета.
Type	Тип пакета IGMP. Тип может быть одним из следующих: Membership Query – запрос членства IGMP V1_Membership_Report – отчёт о членах группы IGMP v 1 V2_Membership_Report – отчёт о членах группы IGMP v 2 V3_Membership_Report – отчёт о членах группы IGMP v 3 V2_Leave_Group – отчет о выходе из группы IGMP v 2
Group	Многоадресный адрес группы в заголовке IGMP.

no debug igmpsnooping transmit

Данная команда отключает отслеживание переданных пакетов IGMP Snooping.

Формат no debug igmpsnooping transmit

Режим Privileged EXEC

debug igmpsnooping packet receive

Эта команда позволяет отслеживать пакеты IGMP Snooping, полученные коммутатором. Snooping должен быть включен на устройстве и интерфейсе для мониторинга пакетов для определенного интерфейса.

По умолчанию отключено

Формат debug igmpsnooping packet receive

Режим Privileged EXEC

ПРИМЕР: вывода сообщения трассировки показан ниже.

<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]: igmp_snooping_debug.c(116) 908 % Pkt RX - Intf: 1/0/20(20), Vlan_Id:1 Src_Mac: 00:03:0e:00:00:10 Dest_Mac: 01:00:5e:00:00:05 Src_IP: 11.1.1.1 Dest_IP: 225.0.0.5 Type: Membership_Query Group: 225.0.0.5

В сообщении трассировки отображаются следующие параметры:

Параметр	Значение
RX	Пакет, полученный устройством.
Intf	Интерфейс, через который пришел пакет. Указывается в формате unit/slot/port (внутренний номер интерфейса). Значение «unit» для коммутаторов не в стеке всегда показывается как 1.
Src_Mac	MAC-адрес источника пакета.
Dest_Mac	Многоадресный MAC-адрес назначения пакета.

Параметр	Значение
Src_IP	IP-адрес источника в заголовке пакета.
Dest_IP	Многоадресный IP-адрес назначения пакета.
Type	Тип пакета IGMP. Тип может быть одним из следующих: Membership Query – запрос членства IGMP V1_Membership_Report – отчёт о членах группы IGMP v 1 V2_Membership_Report – отчёт о членах группы IGMP v 2 V3_Membership_Report – отчёт о членах группы IGMP v 3 V2_Leave_Group – отчет о выходе из группы IGMP v 2
Group	Многоадресный адрес группы в заголовке IGMP.

no debug igmpsnooping receive

Данная команда отключает отслеживание полученных пакетов IGMP Snooping.

Формат no debug igmpsnooping receive

Режим Privileged EXEC

debug ip acl

Используйте эту команду для включения отладки пакетов IP-протокола, соответствующих критериям ACL.

По умолчанию отключено

Формат debug ip acl acl Number

Режим Privileged EXEC

no debug ip acl

Используйте эту команду для отлючения отладки пакетов IP-протокола, соответствующих критериям ACL.

Формат no debug ip acl acl Number

Режим Privileged EXEC

debug lacp packet

Эта команда позволяет отслеживать пакеты LACP, полученные и переданные коммутатором.

По умолчанию отключено

Формат debug lacp packet

Режим Privileged EXEC

ПРИМЕР: вывода сообщения трассировки показан ниже.

<15> JAN 01 14:04:51 10.254.24.31-1

DOT3AD[183697744]: dot3ad_debug.c(385) 58 %% Pkt TX - Intf: 1/0/1(1), Type: LACP, Sys: 00:11:88:14:62:e1, State: 0x47, Key: 0x36

no debug lacp packet

Данная команда отключает отслеживание пакетов LACP.

Формат no debug lacp packet

Режим Privileged EXEC

debug ping packet

Эта команда активирует отслеживание эхо-запросов и ответов ICMP. Команда отслеживает пинг на сетевом или служебном порте при коммутации пакетов. Для маршрутизации пинг отслеживается также на портах маршрутизации.

По умолчанию отключено

Формат debug ping packet

Режим Privileged EXEC

ПРИМЕР: вывода сообщения трассировки показан ниже.

<15> JAN 01 00:21:22 192.168.17.29-1 SIM[181040176]: sim_debug.c(128) 20 % Pkt TX - Intf: 1/0/1(1), SRC_IP:10.50.50.2, DEST_IP:10.50.50.1, Type:ECHO_REQUEST

<15> JAN 01 00:21:22 192.168.17.29-1 SIM[182813968]: sim_debug.c(82) 21 % Pkt RX - Intf: 1/0/1(1), SRC_IP:10.50.50.1, DEST_IP:10.50.50.2, Type:ECHO_REPLY

В сообщении трассировки отображаются следующие параметры:

Параметр	Значение
TX/RX	TX - пакет, переданный устройством. RX - пакет, полученный устройством.
Intf	Интерфейс, через который пришел или вышел пакет. Указывается в формате unit/slot/port (внутренний номер интерфейса). Значение «unit» для коммутаторов не в стеке всегда показывается как 1.
SRC_IP	IP-адрес источника в заголовке пакета.
DEST_IP	IP-адрес назначения в заголовке пакета.
Type	Определяет, является ли ICMP-сообщение REQUEST или RESPONSE.

no debug ping packet

Эта команда отключает отслеживание эхо-запросов и ответов ICMP.

Формат no debug ping packet

Режим Privileged EXEC

debug spanning-tree bpdu

Эта команда позволяет отслеживать spanning tree BPDU, полученные и переданные коммутатором.

По умолчанию отключено

Формат debug spanning-tree bpdu

Режим Privileged EXEC

no debug spanning-tree bpdu

Данная команда отключает отслеживание spanning tree BPDU.

Формат no debug spanning-tree bpdu

Режим Privileged EXEC

debug spanning-tree bpdu receive

Эта команда позволяет отслеживать spanning tree BPDU, полученные коммутатором. Функция Spanning Tree должна быть включен на устройстве и интерфейсе для мониторинга пакетов для определенного интерфейса.

По умолчанию отключено

Формат debug spanning-tree bpdu receive

Режим Privileged EXEC

ПРИМЕР: вывода сообщения трассировки показан ниже.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 % Pkt RX - Intf: 1/
0/9(9), Source_Mac: 00:11:88:4e:c2:10 Version: 3, Root Mac: 00:11:88:4e:c2:00, Root Priority:
0x8000 Path Cost: 0
```

В сообщении трассировки отображаются следующие параметры:

Параметр	Значение
RX	Пакет, полученный устройством.
Intf	Интерфейс, через который пришел пакет. Указывается в формате unit/port/slot (внутренний номер интерфейса). Значение «unit» для коммутаторов не в стеке всегда показывается как 1.
Source_Mac	MAC-адрес источника пакета.
Version	Версия spanning tree protocol (0-3). 0 означает STP, 2 – RSTP, и 3 – MSTP.
Root_Mac	MAC-адрес корневого моста CIST.

Параметр	Значение
Root_Priority	Приоритет корневого моста CIST. Диапазон значений: 0 – 61440. Отображается в шестнадцатеричном формате, кратно 4096.
Path_Cost	Компонент BPDU – внешняя стоимость пути до корня.

no debug spanning-tree bpdu receive

Данная команда отключает отслеживание полученных spanning tree BPDU.

Формат no debug spanning-tree bpdu receive

Режим Privileged EXEC

debug spanning-tree bpdu transmit

Эта команда позволяет отслеживать spanning tree BPDU, отправленные коммутатором. Функция Spanning Tree должна быть включена на устройстве и интерфейсе для мониторинга пакетов для определенного интерфейса.

По умолчанию отключено

Формат debug spanning-tree bpdu transmit

Режим Privileged EXEC

ПРИМЕР: вывода сообщения трассировки показан ниже.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 % Pkt TX - Intf: 1/0/7(7), Source_Mac: 00:11:88:4e:c2:00 Version: 3, Root_Mac: 00:11:88:4e:c2:00, Root_Priority: 0x8000 Path_Cost: 0
```

В сообщении трассировки отображаются следующие параметры:

Параметр	Значение
TX	Пакет, переданный устройством.
Intf	Интерфейс, через который выходит пакет. Указывается в формате unit/port/slot (внутренний номер интерфейса). Значение «unit» для коммутаторов не в стеке всегда показывается как 1.
Source_Mac	MAC-адрес источника пакета.
Version	Версия spanning tree protocol (0-3). 0 означает STP, 2 – RSTP, и 3 – MSTP.
Root_Mac	MAC-адрес корневого моста CIST.
Root_Priority	Приоритет корневого моста CIST. Диапазон значений: 0 – 61440. Отображается в шестнадцатеричном формате, кратно 4096.
Path_Cost	Компонент BPDU – внешняя стоимость пути до корня.

no debug spanning-tree bpdu transmit

Данная команда отключает отслеживание переданных spanning tree BPDU.

Формат no debug spanning-tree bpdu transmit

Режим Privileged EXEC

debug tacacs

Данная команда используется для активации отладки TACACS+.

Формат debug tacacs {packet | authorization | accounting | authentication}

Режим Global Config

Параметр	Описание
packet	Включение отладки пакетов TACACS+.
authorization	Включение отладки авторизации TACACS+.
accounting	Включение отладки учета TACACS+.
authentication	Включение отладки аутентификации TACACS+.

debug transfer

Данная команда включает отладку для передачи файлов.

Формат debug transfer

Режим Privileged EXEC

no debug transfer

Данная команда отключает отладку для передачи файлов.

Формат no debug transfer

Режим Privileged EXEC

show debugging

Данная команда отображает конфигурацию активированных отслеживаний пакетов.

Формат show debugging

Режим Privileged EXEC

ПРИМЕР: Вывод командной строки для данной команды.

```
console# debug arp Arp packet tracing enabled.
console# show debugging Arp packet tracing enabled.
```

exception protocol

Используйте эту команду, чтобы указать протокол, используемый для хранения файла дампа ядра.

По умолчанию Нет

Формат exception protocol {nfs | tftp | ftp | none}

Режим Global Config

no exception protocol

Используйте эту команду для сброса конфигурации протокола до значения по умолчанию.

По умолчанию Нет

Формат no exception protocol

Режим Global Config

exception dump active-port

Эта команда указывает интерфейс для дампа ядра. Это единственный порт, используемый для выгрузки дампа ядра.

По умолчанию Нет

Формат exception dump active-port *unit/slot/port*

Режим Global Config

no exception dump active-port

Эта команда сбрасывает настройки интерфейса для дампа ядра на установки по умолчанию.

По умолчанию Нет

Формат no exception dump active-port

Режим Global Config

exception dump tftp-server

Используйте эту команду для настройки IP-адреса удаленного TFTP-сервера, чтобы выгружать дампы файлов ядра на внешний сервер.

По умолчанию Нет

Формат exception dump tftp-server {*ip-address*}

Режим Global Config

no exception dump tftp-server

Используйте эту команду, чтобы сбросить конфигурацию удаленного сервера для дампов файлов ядра на значения по умолчанию.

По умолчанию Нет

Формат no exception dump tftp-server

Режим Global Config

exception dump nfs

Используйте эту команду для настройки точки монтирования NFS, чтобы выгрузить файл ядра в файловую систему NFS.

По умолчанию Нет

Формат exception dump nfs *ip-address/dir*

Режим Global Config

no exception dump nfs

Используйте эту команду, чтобы сбросить конфигурацию точки монтирования NFS на значения по умолчанию.

По умолчанию Нет

Формат no exception dump nfs

Режим Global Config

exception dump filepath

Используйте эту команду, чтобы настроить путь к дампу файла ядра при выгрузке на TFTP или FTP-сервера, подкаталог точки монтирования NFS.

По умолчанию Нет

Формат exception dump filepath *dir*

Режим Global Config

no exception dump filepath

Используйте эту команду, чтобы сбросить конфигурацию пути к дампу файла ядра на значения по умолчанию.

По умолчанию Нет

Формат no exception dump filepath

Режим Global Config

exception core-file

Используйте эту команду для настройки префикса для имени файла ядра. Имя файла генерируется с префиксом следующим образом:

Если выбрано имя хоста:

file-name-prefix_hostname_Time_Stamp.bin

Если имя хоста не выбрано:

file-name-prefix_MAC_Address_Time_Stamp.bin

Если имя хоста настроено, имя файла ядра содержит имя хоста, в противном случае при создании файла дампа ядра в имени используется MAC-адрес. Длина составляет 15 символов.

По умолчанию Core

Формат exception core-file {*file-name-prefix* | [hostname] | [time-stamp]}

Режим Global Config

no exception core-file

Используйте эту команду, чтобы сбросить конфигурацию префикса файла ядра на значения по умолчанию. Имя хоста и временная отметка отключены.

По умолчанию Core

Формат no exception core-file

Режим Global Config

exception switch-chip-register

Данная команда включает и отключает дамп регистра чипа коммутатора в случае исключения. Дамп регистра чипа коммутатора снимается только для управляющего устройства в стеке.

По умолчанию Отключено

Формат exception switch-chip-register {enable | disable}

Режим Global Config

exception dump ftp-server

Используйте эту команду для настройки IP-адреса удаленного FTP-сервера, чтобы сбрасывать дампы файлов ядра на внешний сервер. Если имя пользователя и пароль не настроены, коммутатор использует анонимный FTP. (Для этого FTP-сервер должен быть настроен на приём анонимного FTP-соединения).

По умолчанию Нет

Формат exception dump ftp-server *ip-address* [{username *user-name* password *password*}]

Режим Global Config

no exception dump ftp-server

Используйте эту команду, чтобы сбросить конфигурацию удаленного FTP-сервера для дампа исключения на значения по умолчанию. Эта команда также сбрасывает имя пользователя и пароль FTP на пустые строки.

По умолчанию Нет

Формат no exception dump ftp-server

Режим Global Config

exception dump compression

Данная команда включает режим сжатия.

По умолчанию Включено

Формат exception dump compression

Режим Global Config

no exception dump compression

Данная команда отключает режим сжатия.

По умолчанию Нет

Формат no exception compression

Режим Global Config

exception dump stack-ip-address protocol

Эта команда настраивает IP-протокол (DHCP или static), который будет использоваться для настройки служебного порта при сбое устройства. Если он настроен как DHCP, то устройство получает IP-адрес с сервера DHCP, доступного в сети.

По умолчанию dhcp

Формат exception dump stack-ip-address protocol {dhcp | static}

Режим Global Config

no exception dump stack-ip-address protocol

Эта команда сбрасывает настройки IP-протокола (DHCP или static) на значения по умолчанию.

По умолчанию Нет

Формат no exception dump stack-ip-address protocol

Режим Global Config

exception dump stack-ip-address add

Эта команда добавляет статический IP-адрес, который должен быть назначен служебному порту отдельного устройства в стеке при сбое коммутатора. Данный IP-адрес используется при выполнении дампа ядра.

По умолчанию Нет

Формат exception dump stack-ip-address add *ip-address netmask* [*gateway*]

Режим Global Config

exception dump stack-ip-address remove

Данная команда удаляет настройки IP-адреса стека. Если этот IP-адрес назначен любому устройству в стеке, этот IP-адрес удаляется из устройства.

По умолчанию Нет

Формат exception dump stack-ip-address remove *ip-address netmask*

Режим Global Config

write core

Данная команда используется для генерации файла дампа ядра по требованию. Команда полезна при тестировании настройки дампа ядра. Например, если настроен TFTP-протокол, **write core test** связывается с сервером TFTP и информирует пользователя о доступности данного сервера. Аналогично, если настроен протокол nfs, эта команда монтирует и размонтирует файловую систему и информирует пользователя о статусе.

ПРИМЕЧАНИЕ: **write core** перезагружает коммутатор, что может быть полезным при некорректной работе устройства (но не его сбое).

Для команды write core test, имя файла назначения используется для теста TFTP. При желании вы можете указать имя файла назначения, если настроен протокол TFTP.

По умолчанию Нет

Формат write core [test [*dest_file_name*]]

Режим Privileged EXEC

debug exception

Данная команда отображает поддержку функций дампа ядра.

По умолчанию Нет

Формат debug exception

Режим Privileged EXEC

show exception

Используйте эту команду, чтобы отобразить параметры конфигурации для генерации файла дампа ядра.

По умолчанию Нет

Формат show exception

Режим Privileged EXEC

ПРИМЕР: Ниже приведен пример выполнения команды. **show exception**

Coredump file name	core
Coredump filename uses hostname	False
Coredump filename uses time-stamp	TRUE
TFTP Server Address	TFTP server configuration
FTP Server IP	FTP server configuration
FTP user name	FTP user name
FTP password	FTP password

NFS Mount point	NFS mount point configuration
File path	Remote file path
Core File name prefix	Core file prefix configuration.
Hostname	Core file name contains hostname if enabled.
Timestamp	Core file name contains timestamp if enabled.
Switch Chip Register Dump	Switch chip register dump configuration
Compression mode	TRUE/FALSE
Active network port	0/28
Stack IP Address Protocol	DHCP/Static
Stack IP Address	List of IP addresses configured

show exception log

Эта команда отображает журнал дампов ядра в локальной файловой системе.

По умолчанию Нет

Формат show exception log [previous]

Режим Privileged EXEC, Config Mode

logging persistent

Данная команда настраивает постоянное журналирование на коммутаторе. Уровень критичности регистрируемых сообщений указывается параметром «severity level». Возможные степени критичности: (emergency|0, alert|1, critical|2, error|3, warning|4, notice|5, info|6, debug|7).

По умолчанию Отключено

Формат logging persistent *severity level*

Режим Global Config

no logging persistent

Данная команда отключает постоянное журналирование на коммутаторе.

Формат no logging persistent

Режим Global Config

mbuf

Используйте эту команду для настройки пороговых значений буфера памяти (MBUF) и генерирования уведомлений при достижении пределов MBUF.

Формат mbuf {falling-threshold | rising threshold | severity}

Режим Global Config

Поле	Описание
Rising Threshold	Верхний порог - процентное значение ресурсов буфера памяти, превышение которого на указанный временной интервал («rising interval») вызывает уведомление. Диапазон - от 1 до 100. Значение по умолчанию - 0 (отключено).
Falling Threshold	Нижний порог - процентное значение ресурсов буфера памяти. Уведомление происходит, когда использование ресурсов падает ниже данного значения на указанный временной интервал. Диапазон - от 1 до 100. Значение по умолчанию - 0 (отключено).
Severity	Уровень критичности, при котором Mbuf регистрирует сообщения. Диапазон - от 1 до 7. Значение по умолчанию – 5 (notice).

show mbuf

Данная команда отображает параметры мониторинга использования буфера памяти (MBUF).

Формат show mbuf

Режим Privileged EXEC

Поле	Описание
Rising Threshold	Верхний порог - процентное значение ресурсов буфера памяти, превышение которого на указанный временной интервал («rising interval») вызывает уведомление. Диапазон - от 1 до 100. Значение по умолчанию - 0 (отключено).
Falling Threshold	Нижний порог - процентное значение ресурсов буфера памяти. Уведомление происходит, когда использование ресурсов падает ниже данного значения на указанный временной интервал. Диапазон - от 1 до 100. Значение по умолчанию - 0 (отключено).
Severity	Уровень критичности.

show mbuf total

Данная команда отображает информацию о буфере памяти (MBUF).

Формат show mbuf total

Режим Privileged EXEC

Поле	Описание
Mbufs Total	Общее количество буферов сообщений в системе.
Mbufs Free	Количество буферов сообщений, доступных в настоящее время.
Mbufs Rx Used	Количество буферов сообщений, используемых в настоящее время.
Total Rx Norm Alloc Attempts	Количество попыток системы предоставить квоту буфера сообщений класса RX Norm.
Total Rx Mid2 Alloc Attempts	Количество попыток системы предоставить квоту буфера сообщений класса RX Mid2
Total Rx Mid1 Alloc Attempts	Количество попыток системы предоставить квоту буфера сообщений класса RX Mid1.
Total Rx Mid0 Alloc Attempts	Количество попыток системы предоставить квоту буфера сообщений класса RX Mid0.
Total Rx High Alloc Attempts	Количество попыток системы предоставить квоту буфера сообщений класса RX High.
Total Tx Alloc Attempts	Количество попыток системы предоставить квоту буфера сообщений класса TX.
Total Rx Norm Alloc Failures	Количество отказов предоставления квоты буфера для сообщений класса RX.
Total Rx Mid2 Alloc Failures	Количество отказов предоставления квоты буфера для сообщений класса RX Mid2.
Total Rx Mid1 Alloc Failures	Количество отказов предоставления квоты буфера для сообщений класса RX Mid1.
Total Rx Mid0 Alloc Failures	Количество отказов предоставления квоты буфера для сообщений класса RX Mid0.
Total Rx High Alloc Failures	Количество отказов предоставления квоты буфера для сообщений класса RX High.
Total Tx Alloc Failures	Количество отказов предоставления квоты буфера для сообщений класса TX.

show msg-queue

Данная команда отображает очереди сообщений.

По умолчанию Нет

Формат show msg-queue

Режим Privileged EXEC

6.15. Команда проверки кабеля

Функция тестирования кабеля позволяет определить состояние физического соединения на выбранном порту.

ПРИМЕЧАНИЕ: Функциональность данной команды поддерживается только для медного кабеля. Для оптических кабелей команда не поддерживаются.

Если на порте во время проверки кабеля установлено активное соединение, оно может прекратиться на время теста.

cablestatus

Данная команда возвращает состояние указанного порта.

Формат cablestatus *unit/slot/port*

Режим Privileged EXEC

Поле	Описание
Cable Status	Команда возвращает одно из следующих состояний: • Normal: Кабель работает корректно. • Open: Кабель отсоединен либо разъем неисправен. • Short: На кабеле обнаружено короткое замыкание. • Cable Test Failed: Не удалось определить состояние кабеля. Кабель при этом может быть в рабочем состоянии. • Crosstalk: На кабеле обнаружены перекрестные помехи. • No Cable: Кабель отсутствует.
Cable Length	Если эта функция поддерживается PHY для текущей скорости связи, длина кабеля отображается как диапазон между наименьшей и наибольшей расчётными длинами. Обратите внимание, что если линия связи отключена и кабель подключен к адаптеру 10/100 Ethernet, то состояние кабеля может отображаться как «Open» или «Short», потому что некоторые адаптеры Ethernet оставляют неиспользуемые пары проводов разомкнутыми или заземленными. Если длину кабеля определить не удаётся, команда возвращает статус «Unknown».

6.16. Команды удаленного мониторинга

Удаленный мониторинг (RMON) представляет собой метод сбора различных данных о сетевом трафике. RMON поддерживает 64-битные счетчики (RFC 3273) и таблицы аварийных оповещений высокой емкости (RFC 3434).

ПРИМЕЧАНИЕ: Конфигурационной команды для статистики Ethernet и High Capacity Ethernet не существует. Источник данных для статистики Ethernet и High Capacity Ethernet настраивается в процессе инициализации.

rmon alarm

Данная команда настраивает запись alarm RMON в группе RMON alarm MIB.

Формат rmon alarm *alarm number variable sample interval* {absolute|delta} rising-threshold

value [rising-event-index] falling-threshold value [falling-event-index] [startup {rising|falling|rising-falling}] [owner string]

Режим Global Config

Параметр	Описание
Alarm Index	Индекс, который однозначно идентифицирует запись в таблице аварийных оповещений. Каждая запись определяет диагностический образец в определенном интервале для объекта на устройстве. Диапазон - от 1 до 65535.
Alarm Variable	Идентификатор объекта конкретной переменной для выборки. Только переменные, которые преобразуются в простой тип числа ASN.1.
Alarm Interval	Интервал в секундах, в течение которого данные отбираются и сравниваются с верхним и нижним порогами. Диапазон от 1 до 2147483647. Значение по умолчанию - 1.
Alarm Absolute Value	Значение статистики в течение последнего периода выборки. Объект доступен только для чтения, 32-битное значение знакового типа.
Alarm Rising Threshold	Верхний порог для выборочной статистики. Диапазон от -2147483648 до 2147483647. Значение по умолчанию - 1.
Alarm Rising Event Index	Индекс записи события, которое используется при превышении верхнего порога. Диапазон - от 1 до 65535. Значение по умолчанию - 1.
Alarm Falling Threshold	Нижний порог для выборочной статистики. Диапазон - от -2147483648 до 2147483647. Значение по умолчанию - 1.
Alarm Falling Event Index	Индекс записи события, которое используется при превышении нижнего порога. Диапазон - от 1 до 65535. Значение по умолчанию - 2.
Alarm Startup Alarm	Оповещение, которое может быть отправлено. Возможные значения: rising, falling либо rising-falling. По умолчанию – rising-falling.

Параметр	Описание
Alarm Owner	Строка владельца, связанная с записью оповещения. По умолчанию: monitorAlarm.

ПРИМЕР: Ниже приведен пример выполнения команды.

(Routing) (Config)# rmon alarm 1 ifInErrors.2 30 absolute rising-threshold 100 1 falling-threshold 10 2 startup rising owner myOwner

no rmon alarm

Данная команда удаляет запись оповещения RMON.

Формат no rmon alarm *alarm number*

Режим Global Config

ПРИМЕР: Ниже приведен пример выполнения команды.

(Routing) (Config)# no rmon alarm 1

rmon hcalarm

Данная команда настраивает запись hcalarm RMON в группе High Capacity RMON alarm MIB.

Формат rmon hcalarm *alarm number variable sample interval* {absolute|delta} rising-threshold high *value* low *value* status {positive|negative} [*rising-event-index*] fallingthreshold high *value* low *value* status {positive|negative} [*falling-event-index*] [startup {*rising*|*falling*|*rising-falling*}] [owner *string*]

Режим Global Config

Параметр	Описание
High Capacity Alarm Index	Произвольное целочисленное значение индекса, используемое для уникальной идентификации записи тревоги высокой емкости. Диапазон - от 1 до 65535.
High Capacity Alarm Variable	Идентификатор объекта конкретной переменной для выборки. Только переменные, которые преобразуются в простой тип числа ASN.1.
High Capacity Alarm interval	Интервал в секундах, в течение которого данные отбираются и сравниваются с верхним и нижним порогами. Диапазон - от 1 до 2147483647. Значение по умолчанию - 1.
High Capacity Alarm Sample Type	Метод выборки конкретной переменной и вычисление значения для сравнения с порогами. Возможные типы: Absolute Value либо Delta Value. Значение по умолчанию – Absolute Value.

Параметр	Описание
High Capacity Alarm Absolute Value	Абсолютное значение (т.е. без знака) статистики hcAlarmVariable в течение последнего периода выборки. Значение текущего периода выборки не будет доступно до окончания периода. Объект доступен только для чтения, 64-битное значение без знака.
High Capacity Alarm Absolute Alarm Status	Этот объект указывает на достоверность и знак данных для объекта абсолютного значения оповещения высокой емкости (hcAlarmAbsValueobject). Возможные типы: valueNotAvailable, valuePositive либо valueNegative. По умолчанию – valueNotAvailable.
High Capacity Alarm Startup Alarm	Оповещение высокой емкости, которое может быть отправлено. Возможные значения: rising, falling либо rising-falling. По умолчанию – rising-falling.
High Capacity Alarm Rising-Threshold Absolute Value Low	Нижние 32 бита абсолютного значения порога для выборочной статистики. Диапазон от 0 до 4294967295. Значение по умолчанию - 1.
High Capacity Alarm Rising-Threshold Absolute Value High	Верхние 32 бита абсолютного значения порога для выборочной статистики. Диапазон от 0 до 4294967295. Значение по умолчанию - 0.
High Capacity Alarm Rising-Threshold Value Status	Этот объект указывает знак данных для верхнего порога, определяемый объектами hcAlarmRisingThresAbsValueLow и hcAlarmRisingThresAbsValueHigh. Возможные типы: valueNotAvailable, valuePositive либо valueNegative. По умолчанию – valuePositive.
High Capacity Alarm Falling-Threshold Absolute Value Low	Нижние 32 бита абсолютного значения порога для выборочной статистики. Диапазон - от 0 до 4294967295. Значение по умолчанию - 1.
High Capacity Alarm Falling-Threshold Absolute Value High	Верхние 32 бита абсолютного значения порога для выборочной статистики. Диапазон - от 0 до 4294967295. Значение по умолчанию - 0.

Параметр	Описание
High Capacity Alarm Falling-Threshold Value Status	Этот объект указывает знак данных для нижнего порога, определяемый объектами hcAlarmFallingThresAbsValueLow и hcAlarmFallingThresAbsValueHigh. Возможные типы: valueNotAvailable, valuePositive либо valueNegative. По умолчанию – valuePositive.
High Capacity Alarm Rising Event Index	Индекс записи события, которое используется при превышении верхнего порога. Диапазон - от 1 до 65535. Значение по умолчанию - 1.
High Capacity Alarm Falling Event Index	Индекс записи события, которое используется при превышении нижнего порога. Диапазон - от 1 до 65535. Значение по умолчанию - 2.
High Capacity Alarm Failed Attempts	Количество раз, когда связанный экземпляр hcAlarmVariable был опрошен от имени hcAlarmEntry (в активном состоянии), и значение не было доступно. Объект доступен только для чтения, 32-битное значение счетчика.
High Capacity Alarm Owner	Строка владельца, связанная с записью оповещения. По умолчанию: monitorHCAlarm.
High Capacity Alarm Storage Type	Тип энергонезависимого хранилища, настроенного для этой записи. Объект доступен только для чтения. По умолчанию – volatile.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)# rmon hcalarm 1 ifInOctets.1 30 absolute rising-threshold high 1 low 100 status positive 1 falling-threshold high 1 low 10 status positive startup rising owner myOwner
```

no rmon hcalarm

Данная команда удаляет запись rmon hcalarm.

Формат no rmon hcalarm alarm number

Режим Global Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)# no rmon hcalarm 1
```

rmon event

Данная команда настраивает запись события RMON event в группе RMON event MIB.

Формат rmon event event number [description string|log|owner string|trap community]

Режим Global Config

Параметр	Описание
Event Index	Индекс, который однозначно идентифицирует запись в таблице событий. Каждая такая запись описывает одно событие, которое должно генерироваться при возникновении соответствующих условий. Диапазон - от 1 до 65535.
Event Description	Комментарий с описанием события. По умолчанию – alarmEvent.
Event Type	Тип уведомления о данном событии. Возможные значения: None, Log, SNMP Trap, Log and SNMP Trap. По умолчанию – None.
Event Owner	Строка владельца, связанная с записью. По умолчанию – monitorEvent.
Event Community	SNMP-сообщество, специфичное для данной строки октетов, используемое для отправки SNMP trap. По умолчанию – public.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)# rmon event 1 log description test
```

no rmon event

Данная команда удаляет запись rmon Event.

Формат no rmon event event number

Режим Global Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)# no rmon Event 1
```

rmon collection history

Данная команда настраивает параметры управления журнала удаленного контроля группы MIB RMON historyControl.

ПРИМЕЧАНИЕ: Команда не поддерживается для диапазона интерфейсов. Каждая запись управления сбором журнала удаленного контроля RMON может быть настроена только на одном интерфейсе. Если вы попытаетесь настроить ее на нескольких интерфейсах, DUT выдаст сообщение об ошибке.

Формат rmon collection history *index number* [buckets *number*|interval *interval in sec*|owner *string*]

Режим Interface Config

Параметр	Описание
History Control Index	Индекс, который однозначно идентифицирует запись в таблице historyControl. Каждая такая запись определяет набор выборок на определенном интервале для интерфейса на устройстве. Диапазон - от 1 до 65535.
History Control Data Source	Интерфейс-источник, для которого собираются данные истории.
History Control Buckets Requested	Запрошенное количество дискретных временных интервалов, по которым должны быть сохранены данные. Диапазон - от 1 до 65535. Значение по умолчанию - 50.
History Control Buckets Granted	Количество дискретных интервалов выборки, через которые должны быть сохранены данные. Объект доступен только для чтения. Значение по умолчанию - 10.
History Control interval	Интервал в секундах, по которому производится выборка данных. Диапазон - от 1 до 3600. Значение по умолчанию - 1800.
History Control Owner	Строка владельца, связанная с записью журнала контроля. Значение по умолчанию - monitorHistoryControl.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Interface 1/0/1)# rmon collection history 1 buckets 10 interval 30 owner myOwner
```

ПРИМЕР: Ниже приведен пример выполнения команды.

(Routing) (Interface 1/0/1-1/0/10)#rmon collection history 1 buckets 10 interval 30 owner myOwner Error: 'rmon collection history' is not supported on range of interfaces.

no rmon collection history

Эта команда удалит запись группы управления журнала контроля с указанным номером индекса.

Формат no rmon collection history *index number*

Режим Interface Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Interface 1/0/1-1/0/10)# no rmon collection history 1
```

show rmon

Эта команда отображает записи в RMON alarm table.

Формат show rmon {alarms | alarm alarm-index}

Режим Privileged EXEC

Параметр	Описание
Alarm Index	Индекс, который однозначно идентифицирует запись в таблице аварийных оповещений. Каждая запись определяет диагностический образец в определенном интервале для объекта на устройстве. Диапазон - от 1 до 65535.
Alarm Variable	Идентификатор объекта конкретной переменной для выборки. Только переменные, которые преобразуются в простой тип числа ASN.1.
Alarm Interval	Интервал в секундах, в течение которого данные отбираются и сравниваются с верхним и нижним порогами. Диапазон - от 1 до 2147483647. Значение по умолчанию - 1.
Alarm Absolute Value	Значение статистики в течение последнего периода выборки. Объект доступен только для чтения, 32-битное значение знакового типа.
Alarm Rising Threshold	Верхний порог для выборочной статистики. Диапазон - от -2147483648 до 2147483647. Значение по умолчанию - 1.
Alarm Rising Event Index	Индекс события - запись, которая используется при превышении верхнего порога. Диапазон - от 1 до 65535. Значение по умолчанию - 1.
Alarm Falling Threshold	Нижний порог для выборочной статистики. Диапазон - от -2147483648 до 2147483647. Значение по умолчанию - 1.
Alarm Falling Event Index	Индекс события - запись, которая используется при превышении нижнего порога. Диапазон - от 1 до 65535. Значение по умолчанию - 2.
Alarm Startup Alarm	Оповещение, которое может быть отправлено. Возможные значения: rising, falling либо rising-falling. По умолчанию – rising-falling.
Alarm Owner	Строка владельца, связанная с записью оповещения. По умолчанию – monitorAlarm.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show rmon alarms
Index  OID     Owner
----------------------------------------------
alarmInterval.1        MibBrowser
alarmInterval.1        MibBrowser
```

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show rmon alarm 1
Alarm 1
----------
OID: alarmInterval.1
Last Sample Value: 1
Interval: 1
Sample Type: absolute
Startup Alarm: rising-falling
Rising Threshold: 1
Falling Threshold: 1
Rising Event: 1
Falling Event: 2
Owner: MibBrowser
```

show rmon collection history

Эта команда отображает записи в RMON History Control table.

Формат show rmon collection history [interfaces unit/slot/port]

Режим Privileged EXEC

Параметр	Описание
History Control Index	Индекс, который однозначно идентифицирует запись в таблице historyControl. Каждая такая запись определяет набор выборок на определенном интервале для интерфейса на устройстве. Диапазон - от 1 до 65535.
History Control Data Source	Интерфейс-источник, для которого собираются данные истории.
History Control Buckets Requested	Запрошенное количество дискретных временных интервалов, по которым должны быть сохранены данные. Диапазон - от 1 до 65535. Значение по умолчанию - 50.
History Control Buckets Granted	Количество дискретных интервалов выборки, через которые должны быть сохранены данные. Объект доступен только для чтения. Значение по умолчанию - 10.
History Control interval	Интервал в секундах, по которому производится выборка данных. Диапазон - от 1 до 3600. Значение по умолчанию - 1800.

Параметр	Описание
History Control Owner	Строка владельца, связанная с записью журнала контроля. Значение по умолчанию - monitorHistoryControl.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show rmon collection history
Index   Interface   Interval  Requested  Granted   Owner          Samples   Samples
-------------------------------------------------------------------------------
1       1/0/1       30        10         10        myowner
2       1/0/1       1800      50         10        monitorHistoryControl
3       1/0/2       30        50         10        monitorHistoryControl
4       1/0/2       1800      50         10        monitorHistoryControl
5       1/0/3       30        50         10        monitorHistoryControl
6       1/0/3       1800      50         10        monitorHistoryControl
7       1/0/4       30        50         10        monitorHistoryControl
8       1/0/4       1800      50         10        monitorHistoryControl
9       1/0/5       30        50         10        monitorHistoryControl
10      1/0/5       1800      50         10        monitorHistoryControl
11      1/0/6       30        50         10        monitorHistoryControl
12      1/0/6       1800      50         10        monitorHistoryControl
13      1/0/7       30        50         10        monitorHistoryControl
14      1/0/7       1800      50         10        monitorHistoryControl
15      1/0/8       30        50         10        monitorHistoryControl
16      1/0/8       1800      50         10        monitorHistoryControl
17      1/0/9       30        50         10        monitorHistoryControl
18      1/0/9       1800      50         10        monitorHistoryControl
19      1/0/10      30        50         10        monitorHistoryControl
More or (q)uit
```

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show rmon collection history interfaces 1/0/1

Index   Interface   Interval   Requested Samples   Granted Samples   Owner
-------------------------------------------------------------------------------
1       1/0/1       30         10                  10                myowner
2       1/0/1       1800       50                  10                monitorHistoryControl
```

show rmon events

Эта команда отображает записи в RMON Event table.

Формат show rmon events

Режим Privileged EXEC

Параметр	Описание
Event Index	Индекс, который однозначно идентифицирует запись в таблице событий. Каждая такая запись описывает одно событие, которое должно генерироваться при возникновении соответствующих условий. Диапазон - от 1 до 65535.
Event Description	Комментарий с описанием события. По умолчанию – alarmEvent.
Event Type	Тип уведомления, которое зонд делает о данном событии. Возможные значения: None, Log, SNMP Trap, Log and SNMP Trap. По умолчанию – None.
Event Community	SNMP-сообщество, специфичное для данной строки октетов, используемое для отправки SNMP trap. По умолчанию – public.
Owner	Владелец события. Строка владельца, связанная с записью.
Last time sent	Последний раз, когда генерировались запись журнала или сообщение SNMP trap.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) # show rmon events

Index   Description   Type   Community   Owner   Last time sent
-------------------------------------------------------------------------------
1       test          log    public      MIB     0 days 0 h:0 m:0 s
```

show rmon history

Эта команда отображает указанные записи в таблице RMON History table.

Формат show rmon history *index* {errors [period *seconds*]|other [period *seconds*]|throughput [period *seconds*]}

Режим Privileged EXEC

Параметр	Описание
History Control Index	Индекс, который однозначно идентифицирует запись в таблице historyControl. Каждая такая запись определяет набор выборок на определенном интервале для интерфейса на устройстве. Диапазон - от 1 до 65535.
History Control Data Source	Интерфейс-источник, для которого собираются данные истории.
History Control Buckets Requested	Запрошенное количество дискретных временных интервалов, по которым должны быть сохранены данные. Диапазон – от 1 до 65535. Значение по умолчанию - 50.
History Control Buckets Granted	Количество дискретных интервалов выборки, по которым должны быть сохранены данные. Объект доступен только для чтения. Значение по умолчанию - 10.
History Control interval	Интервал в секундах, по которому производится выборка данных. Диапазон - от 1 до 3600. Значение по умолчанию - 1800.
History Control Owner	Строка владельца, связанная с записью журнала контроля. Значение по умолчанию - monitorHistoryControl.
Maximum Table Size	Максимальное количество записей, которые может храниться в таблице истории.
Time	Время, в течение которого собирается образец (в секундах)
CRC Align	Количество ошибок CRC align.
Undersize Packets	Общее количество пакетов неполного размера. Пакеты длиной менее 64 октетов (не включая биты кадрирования, включая октеты FCS).
Oversize Packets	Общее количество пакетов избыточного размера. Пакеты длиной более 1518 октетов (не включая биты кадрирования, включая октеты FCS).
Fragments	Общее количество фрагментированных пакетов. Пакеты, имеющие в длину нецелое количество октетов, либо имеющие неверную FCS (Frame Check Sequence), а также имеющие длину менее 64 октетов (не включая биты кадрирования, включая октеты FCS).

Параметр	Описание
Jabbers	Общее количество пакетов с неверной длиной и контрольной суммой. Пакеты длиной более 1518 октетов (не включая биты кадрирования, включая октеты FCS), а также имеющие в длину нецелое количество октетов, либо имеющие плохую FCS (Frame Check Sequence).
Octets	Общее количество октетов, полученных на интерфейсе.
Packets	Общее количество пакетов (в том числе с ошибками), полученных на интерфейсе.
Broadcast	Общее количество корректных широковещательных пакетов, полученных на интерфейсе.
Multicast	Общее количество корректных многоадресных пакетов, полученных на интерфейсе.
Util	Использование порта интерфейса, связанного с указанным индексом истории.
Dropped Collisions	Общее количество отброшенных коллизий.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show rmon history 1 errors
Sample set: 1  Owner: myowner
Interface: 1/0/1          Interval: 30
Requested Samples: 10     Granted Samples: 10
Maximum table size: 1758
```

Time	CRC Align	Undersize	Oversize	Fragments	Jabbers
Jan 01 1970 21:41:43	0	0	0	0	0
Jan 01 1970 21:42:14	0	0	0	0	0
Jan 01 1970 21:42:44	0	0	0	0	0
Jan 01 1970 21:43:14	0	0	0	0	0
Jan 01 1970 21:43:44	0	0	0	0	0
Jan 01 1970 21:44:14	0	0	0	0	0
Jan 01 1970 21:44:45	0	0	0	0	0
Jan 01 1970 21:45:15	0	0	0	0	0

Jan 01 1970 21:45:45	0	0	0	0	0
Jan 01 1970 21:46:15	0	0	0	0	0

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show rmon history 1 throughput
Sample set: 1  Owner: myowner
Interface: 1/0/1          Interval: 30
Requested Samples: 10     Granted Samples: 10
Maximum table size: 1758
```

Time	Octets	Packets	Broadcast	Multicast	Util
Jan 01 1970 21:41:43	0	0	0	0	1
Jan 01 1970 21:42:14	0	0	0	0	1
Jan 01 1970 21:42:44	0	0	0	0	1
Jan 01 1970 21:43:14	0	0	0	0	1
Jan 01 1970 21:43:44	0	0	0	0	1
Jan 01 1970 21:44:14	0	0	0	0	1
Jan 01 1970 21:44:45	0	0	0	0	1
Jan 01 1970 21:45:15	0	0	0	0	1
Jan 01 1970 21:45:45	0	0	0	0	1
Jan 01 1970 21:46:15	0	0	0	0	1

```
(Routing) #show rmon history 1 other
Sample set: 1             Owner: myowner
Interface: 1/0/1          Interval: 30
Requested Samples: 10     Granted Samples: 10
Maximum table size: 1758
```

Time	Dropped	Collisions
Jan 01 1970 21:41:43	0	0
Jan 01 1970 21:42:14	0	0
Jan 01 1970 21:42:44	0	0
Jan 01 1970 21:43:14	0	0
Jan 01 1970 21:43:44	0	0
Jan 01 1970 21:44:14	0	0

```
Jan 01 1970 21:44:45        0           0
Jan 01 1970 21:45:15        0           0
Jan 01 1970 21:45:45        0           0
Jan 01 1970 21:46:15        0           0
```

show rmon log

Эта команда отображает записи RMON log table.

Формат show rmon log [event-index]

Режим Privileged EXEC

Параметр	Описание
Maximum table size	Максимальное количество записей, которые может храниться в таблице журнала.
Event	Индекс событий, для которых генерируются записи журнала.
Description	Комментарий с описанием события, для которого сгенерирована запись в журнале.
Time	Время генерирации события.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show rmon log
Event   Description    Time
```

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show rmon log 1
Maximum table size: 10
Event   Description    Time
```

show rmon statistics interfaces

Данная команда отображает статистику RMON для указанного интерфейса.

Формат show rmon statistics interfaces *unit/slot/port*

Режим Privileged EXEC

Параметр	Значение
Port	unit/slot/port
Dropped	Общее количество отброшенных событий на интерфейсе.
Octets	Общее количество октетов, полученных на интерфейсе.

Параметр	Значение
Packets	Общее количество пакетов (в том числе ошибочных), полученных на интерфейсе.
Broadcast	Общее количество корректных широковещательных пакетов, полученных на интерфейсе.
Multicast	Общее количество корректных многоадресных пакетов, полученных на интерфейсе.
CRC Align Errors	Общее количество принятых пакетов (исключая биты кадрирования, включая октеты FCS), имеющих длину от 64 до 1518 октетов включительно с ошибкой CRC.
Collisions	Общее количество коллизий на интерфейсе.
Undersize Pkts	Общее количество пакетов неполного размера. Пакеты длиной менее 64 октетов (не включая биты кадрирования, включая октеты FCS).
Oversize Pkts	Общее количество пакетов избыточного размера. Пакеты длиной более 1518 октетов (не включая биты кадрирования, включая октеты FCS).
Fragments	Общее количество фрагментированных пакетов. Пакеты, имеющие в длину нецелое количество октетов, либо имеющие неверную FCS (Frame Check Sequence), а также имеющие длину менее 64 октетов (не включая биты кадрирования, включая октеты FCS).
Jabbers	Общее количество пакетов с неверной длиной и контрольной суммой. Пакеты длиной более 1518 октетов (не включая биты кадрирования, включая октеты FCS), а также имеющие в длину нецелое количество октетов, либо имеющие плохую FCS (Frame Check Sequence).
64 Octets	Общее количество пакетов (исключая биты кадрирования, включая октеты FCS), имеющих длину в 64 октета. включительно.
65-127 Octets	Общее количество пакетов (исключая биты кадрирования, включая октеты FCS), имеющих длину от 65 до 127 октетов.
128-255 Octets	Общее количество пакетов (исключая биты кадрирования, включая октеты FCS), имеющих длину от 128 до 255 октетов.
256-511 Octets	Общее количество пакетов (исключая биты кадрирования, включая октеты FCS), имеющих длину от 256 до 511 октетов.

Параметр	Значение
512-1023 Octets	Общее количество пакетов (исключая биты кадрирования, включая октеты FCS), имеющих длину от 512 до 1023 октетов.
1024-1518 Octets	Общее количество пакетов (исключая биты кадрирования, включая октеты FCS), имеющих длину от 1024 до 1518 октетов.
HC Overflow Pkts	Общее количество пакетов HC overflow.
HC Overflow Octets	Общее количество октетов HC overflow.
HC Overflow Pkts 64 Octets	Общее количество пакетов HC overflow длиной 64 октета.
HC Overflow Pkts 65 - 127 Octets	Общее количество пакетов HC overflow длиной от 65 до 127 октетов.
HC Overflow Pkts 128 - 255 Octets	Общее количество пакетов HC overflow длиной от 128 до 255 октетов.
HC Overflow Pkts 256 - 511 Octets	Общее количество пакетов HC overflow длиной от 256 до 511 октетов.
HC Overflow Pkts 512 - 1023 Octets	Общее количество пакетов HC overflow длиной от 512 до 1023 октетов.
HC Overflow Pkts 1024 - 1518 Octets	Общее количество пакетов HC overflow длиной от 1024 до 1518 октетов.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) # show rmon statistics interfaces 1/0/1
Port: 1/0/1
Dropped:                0
Octets:                 0
Packets:                0
Broadcast:              0
Multicast:              0
CRC Align Errors:       0
```

Collisions:	0
Undersize Pkts:	0
Oversize Pkts:	0
Fragments:	0
Jabbers:	0
64 Octets:	0
65 - 127 Octets:	0
128 - 255 Octets:	0
256 - 511 Octets:	0
512 - 1023 Octets:	0
1024 - 1518 Octets:	0
HC Overflow Pkts:	0
HC Pkts:	0
HC Overflow Octets:	0
HC Octets:	0
HC Overflow Pkts 64 Octets:	0
HC Pkts 64 Octets:	0
HC Overflow Pkts 65 - 127 Octets:	0
HC Pkts 65 - 127 Octets:	0
HC Overflow Pkts 128 - 255 Octets:	0
HC Pkts 128 - 255 Octets:	0
HC Overflow Pkts 256 - 511 Octets:	0
HC Pkts 256 - 511 Octets:	0
HC Overflow Pkts 512 - 1023 Octets:	0
HC Pkts 512 - 1023 Octets:	0
HC Overflow Pkts 1024 - 1518 Octets:	0
HC Pkts 1024 - 1518 Octets:	0

show rmon hcalarms

Эта команда отображает записи в RMON High Capacity alarm table.

Формат show rmon {hcalarms|hcalarm alarm index}

Режим Privileged EXEC

Параметр	Описание
High Capacity Alarm Index	Произвольное целочисленное значение индекса, используемое для уникальной идентификации записи тревоги высокой емкости. Диапазон - от 1 до 65535.

Параметр	Описание
High Capacity Alarm Variable	Идентификатор объекта конкретной переменной для выборки. Только переменные, которые преобразуются в простой тип числа ASN.1.
High Capacity Alarm interval	Интервал в секундах, в течение которого данные отбираются и сравниваются с верхним и нижним порогами. Диапазон - от 1 до 2147483647. Значение по умолчанию - 1.
High Capacity Alarm Sample Type	Метод выборки конкретной переменной и вычисление значения для сравнения порогами. Возможные типы: Absolute Value либо Delta Value. Значение по умолчанию – Absolute Value.
High Capacity Alarm Absolute Value	Абсолютное значение (т.е. без знака) статистики hcAlarmVariable в течение последнего периода выборки. Значение текущего периода выборки не будет доступно до окончания периода. Объект доступен только для чтения, 64-битное значение без знака.
High Capacity Alarm Absolute Alarm Status	Этот объект указывает на достоверность и знак данных для объекта абсолютного значения оповещения высокой емкости (hcAlarmAbsValueobject). Возможные типы: valueNotAvailable, valuePositive либо valueNegative. По умолчанию – valueNotAvailable.
High Capacity Alarm Startup Alarm	Оповещение высокой емкости, которое может быть отправлено. Возможные значения: rising, falling либо rising-falling. По умолчанию – rising-falling.
High Capacity Alarm Rising-Threshold Absolute Value Low	Нижние 32 бита абсолютного значения порога для выборочной статистики. Диапазон - от 0 до 4294967295. Значение по умолчанию - 1.
High Capacity Alarm Rising-Threshold Absolute Value High	Верхние 32 бита абсолютного значения порога для выборочной статистики. Диапазон - от 0 до 4294967295. Значение по умолчанию - 0.
High Capacity Alarm RisingThreshold Value Status	Этот объект указывает знак данных для верхнего порога, определяемый объектами hcAlarmRisingThresAbsValueLow и hcAlarmRisingThresAbsValueHigh. Возможные типы: valueNotAvailable, valuePositive либо valueNegative. По умолчанию – valuePositive.

Параметр	Описание
High Capacity Alarm Falling-Threshold Absolute Value Low	Нижние 32 бита абсолютного значения порога для выборочной статистики. Диапазон - от 0 до 4294967295. Значение по умолчанию - 1.
High Capacity Alarm Falling-Threshold Absolute Value High	Верхние 32 бита абсолютного значения порога для выборочной статистики. Диапазон - от 0 до 4294967295. Значение по умолчанию - 0.
High Capacity Alarm FallingThreshold Value Status	Этот объект указывает знак данных для нижнего порога, определяемый объектами hcAlarmFallingThresAbsValueLow и hcAlarmFallingThresAbsValueHigh. Возможные типы: valueNotAvailable, valuePositive либо valueNegative. По умолчанию – valuePositive.
High Capacity Alarm Rising Event Index	Индекс записи события, которое используется при превышении верхнего порога. Диапазон - от 1 до 65535. Значение по умолчанию - 1.
High Capacity Alarm Falling Event Index	Индекс записи события, которое используется при превышении нижнего порога. Диапазон - от 1 до 65535. Значение по умолчанию - 2.
High Capacity Alarm Failed Attempts	Количество раз, когда связанный экземпляр hcAlarmVariable был опрошен от имени hcAlarmEntry (в активном состоянии), и значение не было доступно. Объект доступен только для чтения, 32-битное значение счетчика.
High Capacity Alarm Owner	Строка владельца, связанная с записью оповещения. По умолчанию – monitorHCAlarm.
High Capacity Alarm Storage Type	Тип энергонезависимого хранилища, настроенного для этой записи. Объект доступен только для чтения. По умолчанию – volatile.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show rmon hcalarms
Index  OID     Owner
-----------------------------------------------
alarmInterval.1        MibBrowser
alarmInterval.1        MibBrowser
```

(Routing) #show rmon hcalarm 1

Alarm 1

OID: alarmInterval.1

Last Sample Value: 1

Interval: 1

Sample Type: absolute

Startup Alarm: rising-falling

Rising Threshold High: 0

Rising Threshold Low: 1

Rising Threshold Status: Positive

Falling Threshold High: 0

Falling Threshold Low: 1

Falling Threshold Status: Positive

Rising Event: 1

Falling Event: 2

Startup Alarm: Rising-Falling

Owner: MibBrowser

6.17. Команды приложения статистики

Приложение статистики дает вам возможность запрашивать статистику использования портов, на основе потоков и приема пакетов в программируемых временных слотах. Приложение статистики собирает статистику за настраиваемый временной диапазон. Вы можете указать номер порта или диапазон портов для отображения статистики. Установленный временной диапазон применяется ко всем портам. Подробная статистика собирается в пределах указанного временного диапазона в формате даты и времени. Вы можете определить временной диапазон в абсолютных и/или периодических значениях. Например, вы можете включить сбор и отображение статистики между 9:00 12 NOV 2011 (START) и 21:00 12 NOV 2012 (END), или же каждый понедельник, среду и пятницу с 9:00 (START) до 21:00 (END).

Статистику можно получить следующими способами:

Пользовательский запрос набора значений счётчиков через консоль.

Через syslog или оповещения по электронной почте. Периодические оповещения через syslog или электронную почту, приходящие в конце периода сбора статистики (END).

Вы можете настроить устройство для отображения статистики в консоли. Собранная статистика отображается в консоли в конце периода сбора статистики (END).

stats group

Эта команда создает новую группу с указанным идентификатором или именем, и настраивает временной диапазон и механизм передачи сообщений для этой группы.

Формат stats group {group id|name} timerange time range name reporting list of reporting methods

Режим Global Config

Параметр	Описание
group ID, name	Имя группы статистики или ее идентификатор для применения на интерфейсе. Диапазон: 1. Received (получено) 2. Received-errors (получено с ошибками) 3. Transmitted (отправлено) 4. Transmitted-errors (отправлено с ошибками) 5. Received-transmitted (получено и отправлено) 6. Port-utilization (использование порта) 7. Congestion (перегрузка) 8. По умолчанию – None.
time range name	Название временного диапазона для группы или правила, основанного на потоке. Диапазон - от 1 до 31 символов (буквы и цифры). По умолчанию – None.
list of reporting methods	Метод передачи информации статистики. Диапазон: None (нет) 1. Console (в консоль) 2. syslog (в журнал) 3. e-mail (на электронную почту) 4. По умолчанию – None.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)# stats group received timerange test reporting console email syslog
(Routing) (Config)# stats group received-errors timerange test reporting email syslog (Routing) (Config)# stats group received-  transmitted timerange test reporting none
```

no stats group

Эта команда удаляет настроенную группу.

Формат no stats group group id|name

Режим Global Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)# no stats group received
(Routing) (Config)# no stats group received-errors
(Routing) (Config)# no stats group received-transmitted
```

stats flow-based

Эта команда настраивает правила статистики, основанные на потоке, для заданных параметров в течение заданного интервала времени. В качестве IP-адресов источника и назначения разрешен только IPv4-адрес.

Формат stats flow-based *rule-id* timerange *time range name* [{srcip *ip-address*} {dstip *ipaddress*} {srcmac *mac-address*} {dstmac *mac-address*} {srctcpport *portid*} {dsttcpport *portid*} {srcudpport *portid*} {dstudpport *portid*}]

Режим Global Config

Параметр	Описание
rule ID	ID правила, основанного на потоке. Диапазон - от 1 до 16. По умолчанию – нет.
time range name	Название временного диапазона для группы или правила, основанного на потоке. Диапазон - от 1 до 31 символов (буквы и цифры). По умолчанию – нет.
srcip ip-address	IP-адрес источника.
dstip ip-address	IP-адрес назначения.
srcmac macaddress	MAC-адрес источника.
dstmac macaddress	MAC-адрес назначения.
srctcpport portid	Номер TCP-порта источника.
dsttcpport portid	Номер TCP-порта назначения.
srcudpport portid	Номер UDP-порта источника.
dstudpport portid	Номер UDP-порта назначения.

ПРИМЕР: Ниже приведен пример выполнения команды.

(Routing) (Config)#stats flow-based 1 timerange test srcip 1.1.1.1 dstip 2.2.2.2 srcmac 1234 dstmac

1234 srctcpport 123 dsttcpport 123 srcudpport 123 dstudpport 123

(Routing) (Config)#stats flow-based 2 timerange test srcip 1.1.1.1 dstip 2.2.2.2 srctcpport 123 dsttcpport 123 srcudpport 123 dstudpport 123

no stats flow-based

Данная команда удаляет статистику на основе потока.

Формат stats flow-based *rule-id*

Режим Global Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)# no stats flow-based 1
(Routing) (Config)# no stats flow-based 2
```

stats flow-based reporting

Эта команда настраивает механизм передачи сообщений для всех правил на основе потока, настроенных в системе. Отдельных механизмов передачи сообщений для каждого правила на основе потока не предусмотрено. Установка механизма передачи сообщений на **none** сбрасывает все механизмы передачи сообщений.

Формат stats flow-based reporting *list of reporting methods*

Режим Global Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)# stats flow-based reporting console email syslog
(Routing) (Config)# stats flow-based reporting email syslog
(Routing) (Config)# stats flow-based reporting none
```

stats group

Данная команда применяет указанную группу к интерфейсу или диапазону интерфейсов.

Формат stats group <group id | name>

Режим Interface Config

Параметр	Описание
group id	Уникальный идентификатор группы.
name	Название группы.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Interface 1/0/1-1/0/10)# stats group 1 (Routing) (Interface 1/0/1-1/0/10)# stats group 2
```

no stats group

Эта команда удаляет интерфейс или диапазон интерфейса из указанной группы.

Формат no stats group <group id | name>

Режим Interface Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Interface 1/0/1-1/0/10)# no stats group 1
(Routing) (Interface 1/0/1-1/0/10)# no stats group 2
```

stats flow-based

Данная команда применяет правило на основе потока, указанное по ID, к интерфейсу или диапазону интерфейсов.

Формат stats flow-based < rule-id>

Режим Interface Config

Параметр	Описание
rule-id	Уникальный идентификатор правила на основе потока.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Interface 1/0/1-1/0/10)# stats flow-based 1
(Routing) (Interface 1/0/1-1/0/10)# stats flow-based 2
```

no stats flow-based

Эта команда удаляет интерфейс или диапазон интерфейса из указанного правила на основе потока.

Формат no stats flow-based <rule-id>

Режим Interface Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Interface 1/0/1-1/0/10)# no stats flow-based 1
(Routing) (Interface 1/0/1-1/0/10)# no stats flow-based 2
```

show stats group

Данная команда отображает настроенный временной диапазон и список интерфейсов для указанной группы, и показывает собранную статистику для заданного временного диапазона с указанным названием интерейса, после завершения данного временного диапазона.

Формат show stats group <group id | name>

Режим Privileged EXEC

Параметр	Описание
group id	Уникальный идентификатор группы.
name	Название группы.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show stats group received
Group: received
Time Range: test
```

Interface List

1/0/2, 1/0/4, lag 1

Counter ID	Interface	Counter Value
Rx Total	1/0/2	951600
Rx Total	1/0/4	304512
Rx Total	lag 1	0
Rx 64	1/0/2	0
Rx 64	1/0/4	4758
Rx 64	lag 1	0
Rx 65to128	1/0/2	0
Rx 65to128	1/0/4	0
Rx 65to128	lag 1	0
Rx 128to255	1/0/2	4758
Rx 128to255	1/0/4	0
Rx 128to255	lag 1	0
Rx 256to511	1/0/2	0

ПРИМЕР: Вывод командной строки для данной команды.

(Routing) #show stats group port-utilization

Group: port-utilization

Time Range: test

Interface List

1/0/2, 1/0/4, lag 1

Interface Utilization (%)

--- ---

1/0/2 0 1/0/4 0 lag 1 0

show stats flow-based

Эта команда отображает настроенный временной диапазон, параметры правил на основе потока и список интерфейсов для указанного потока.

Формат show stats flow-based rule-id|all

Режим Privileged EXEC

Параметр	Описание
rule-id	Уникальный идентификатор правила на основе потока.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show stats flow-based all
Flow based rule Id .....1
Time Range .....test
Source IP .....1.1.1.1
Source MAC .....1234
Source TCP Port.....123
Source UDP Port.....123
Destination IP.....2.2.2.2
Destination MAC.....1234
Destination TCP Port .....123
Destination UDP Port .....123

Interface List
-------------
1/0/1 - 1/0/2

Interface  Hit Count
---------  ---------
1/0/1    100
1/0/2    0

Flow based rule Id .....2
Time Range .....test
Source IP .....1.1.1.1
Source TCP Port.....123
Source UDP Port.....123
Destination IP.....2.2.2.2
Destination TCP Port .....123
Destination UDP Port .....123
Interface List
-------------
1/0/1 - 1/0/2
```

```
Interface  Hit Count
---------  ---------
1/0/1      100
1/0/2      0
```

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show stats flow-based 2
Flow based rule Id .....2
Time Range .....test
Source IP .....1.1.1.1
Source TCP Port.....123
Source UDP Port.....123
Destination IP.....2.2.2.2
Destination TCP Port.....123
Destination UDP Port.....123

Interface List
-------------
1/0/1 - 1/0/2

Interface  Hit Count
---------  ---------
1/0/1      100
1/0/2      0
```

7. РАЗДЕЛ: КОМАНДЫ КОММУТАЦИИ

В этом разделе описываются команды коммутации. Раздел состоит из следующих глав:

- Команды конфигурации порта
- Команды STP (Spanning Tree Protocol)
- Команды VLAN
- Команды частных VLAN
- Команды Voice VLAN
- Команды Provisioning (IEEE 802.1p)
- Команды GARP
- Команды GVRP
- Команды GMRP
- Команды управления сетевым доступом на основе порта
- Команды запрашивающего устройства 802.1X
- Команды Storm-Control
- Команды Port-Channel/LAG (802.3ad)
- Команды зеркалирования портов
- Команды статической фильтрации MAC-адресов
- Команды конфигурации DHCP Snooping
- Команды конфигурации IGMP Snooping
- Команды конфигурации IGMP Snooping Querier
- Команды Port Security
- Команды LLDP (802.1AB)
- Команды LLDP-MED
- Команды Denial of Service
- Команды базы данных MAC

ВНИМАНИЕ: В ДАННОМ РАЗДЕЛЕ КОМАНДЫ ДЕЛЯТСЯ НА ТРИ ФУНКЦИОНАЛЬНЫЕ ГРУППЫ:

1. Команды Show отображают настройки коммутатора, статистику и прочую информацию.
2. Команды конфигурации вносят изменения в настройки коммутатора. Каждой команде конфигурации соответствует команда информации, показывающая текущие настройки.
3. Команды Clear сбрасывают определенные настройки на заводские значения.

7.1. Команды конфигурации порта

В этом разделе описаны команды, которые используются для настройки портов и получения информации об этих портах.

interface

Данная команда предоставляет доступ к режиму Interface Config, который позволяет вам активировать или изменять работу интерфейса (порта). Вы также можете указать диапазон портов (начальный и конечный **unit/slot/port** через дефис).

Формат interface {unit/slot/port | unit/slot/port(startrange)-unit/slot/port(endrange)}

Режим Global Config

ПРИМЕР: Пользователь входит в режим Interface Config для порта 1/0/1:

```
(switch) #configure
(switch) (config)#interface 1/0/1
(switch) (interface 1/0/1)#
```

ПРИМЕР: Пользователь входит в режим Interface Config для портов в диапазоне от 1/0/1 до 1/0/4:

```
(switch) #configure
(switch) (config)#interface 1/0/1-1/0/4
(switch) (interface 1/0/1-1/0/4)#
```

auto-negotiate

Данная команда активирует автоматическое согласование на порту либо на диапазоне портов.

По умолчанию включено

Формат auto-negotiate

Режим Interface Config

no auto-negotiate

Данная команда отключает автоматическое согласование на порту либо на диапазоне портов.

ПРИМЕЧАНИЕ: Автоматическое распознавание отключается, когда автоматическое согласование отключено.

Формат no auto-negotiate

Режим Interface Config

auto-negotiate all

Данная команда активирует автоматическое согласование на всех портах.

По умолчанию включено

Формат auto-negotiate all

Режим Global Config

no auto-negotiate all

Данная команда отключает автоматическое согласование на всех портах.

Формат no auto-negotiate all

Режим Global Config

description

Данная команда позволяет добавить описание интерфейса либо диапазона интерфейсов. Описание может содержать буквы и цифры.

Формат description description

Режим Interface Config

media-type

Данная команда позволяет переключаться между разными режимами комбо-порта (оптическим и медным).

- Combo Port: Порт или интерфейс, который может работать либо в оптическом, либо «медном» режиме.
- Copper and Fiber port: Порт, предназначенный для передачи данных по медному кабелю (например, порт RJ45). Оптический порт в качестве среды передачи данных использует оптический кабель (например, порт SFP).

По умолчанию Auto-select, SFP preferred

Формат media-type {auto-select | rj45 | sfp }

Режим Interface Config

Команда **media-type** поддерживает следующие режимы.

- Auto-select, SFP preferred: Среда передачи данных выбирается автоматически, в зависимости от типа подключенного кабеля. Однако, если подключены оба типа кабеля, предпочтение отдаётся оптическому.
- Auto-select, RJ45 preferred: Среда передачи данных выбирается автоматически, в зависимости от типа подключенного кабеля. Однако, если подключены оба типа кабеля, предпочтение отдаётся медному.
- SFP: Работает только оптический интерфейс. Медный интерфейс не работает в любом случае.
- RJ45: Работает только медный интерфейс. Оптический интерфейс не работает в любом случае.

no media-type

Данная команда сбрасывает настройки media-type на значения по умолчанию.

Формат no media-type

Режим Interface Config

mtu

Данная команда устанавливает размер MTU (Maximum Transmission Unit) в байтах для входящих и исходящих фреймов. Этой командой вы можете настроить поддержку jumbo-фреймов для физических интерфейсов и интерфейсов port-channel (LAG). В стандартной

реализации, размер MTU является действительным целым числом в диапазоне 1522 – 9216 для тегированных пакетов и в диапазоне 1518 – 9216 для нетегированных пакетов.

ПРИМЕЧАНИЕ: Для получения и обработки пакетов MTU Ethernet должен включать любые дополнительные байты, которые могут потребоваться для заголовков уровня 2 OSI. Чтобы настроить размер IP-MTU, являющийся максимальным размером IP-пакета (IP-заголовок + полезные данные), см. “ip mtu”.

По умолчанию	1518 (для нетегированных пакетов)
Формат	mtu 1518-12288
Режим	Interface Config

no mtu

Данная команда сбрасывает размер MTU на настройки по умолчанию.

Формат	no mtu
Режим	Interface Config

shutdown

Данная команда отключает порт либо диапазон портов.

ПРИМЕЧАНИЕ: Команда shutdown может использоваться для отключения физических интерфейсов и интерфейсов port-channel (LAG), но не интерфейсов маршрутизации VLAN.

По умолчанию	включено
Формат	shutdown
Режим	Interface Config

no shutdown

Данная команда активирует порт.

Формат	no shutdown
Режим	Interface Config

shutdown all

Данная команда отключает все порты.

ПРИМЕЧАНИЕ: Команда shutdown all может использоваться для отключения физических интерфейсов и интерфейсов port-channel (LAG), но не интерфейсов маршрутизации VLAN.

По умолчанию	включено
Формат	shutdown all
Режим	Global Config

no shutdown all

Данная команда включает все порты.

Формат no shutdown all

Режим Global Config

speed

Используйте эту команду для включения или отключения автоматического согласования и установки скорости, которая будет анонсироваться этим портом. Параметр «duplex» позволяет настроить анонсирование скорости для режимов half duplex и full duplex.

Ключевое слово auto включает автосогласование на порте. Использование команды без ключевого слова auto, напротив, позволяет убедиться, что автосогласование отключено, и настроить скорость порта согласно значениям команды. При отключенном автосогласовании необходимо настроить скорость и дуплексный режим.

По умолчанию Автосогласование включено.

Формат speed {auto {40G | 10G | 1000 | 100 | 10} [40G | 10G | 1000 | 100 | 10] [half-duplex | full-duplex] | {40G | 10G | 1000 | 100 | 10} {half-duplex | full-duplex}}

Режим Interface Config

speed all

Данная команда настраивает скорость и дуплексный режим для всех интерфейсов.

Формат speed all {100 | 10} {half-duplex | full-duplex}

Режим Global Config

show interface media-type

Данная команда отображает настройки среды передачи данных для указанного интерфейса.

Формат show interface media-type

Режим Privileged EXEC

Отображается следующая информация.

Термин	Значение
Port	Интерфейс в формате unit/slot/port.
Configured Media Type	Тип среды передачи данных интерфейса. auto-select — тип среды выбирается автоматически. Отображается тип среды, имеющий более высокий приоритет. RJ45 — RJ45 SFP — SFP
Active	Отображает текущее состояние комбо-порта.

ПРИМЕР: Ниже приведен пример вывода команды:

```
(Routing) #show interface media-type
```

```
Port       Configured Media Type          Active
---------  -------------------------- ------
0/21       SFP                        RJ45
0/22       auto-select, SFP preferred Down
0/23       auto-select, SFP preferred RJ45
0/24       auto-select, SFP preferred Down
```

show port

Данная команда предоставляет информацию о порте.

Формат show port {*intf-range* | all}

Режим Privileged EXEC

Параметр	Значение
Interface	unit/slot/port
Type	Если данное поле не пустое, оно указывает тип порта. Возможные значения: • Mirror — порт мониторинга. Для получения дополнительной информации см. раздел "Команды зеркалирования портов". • PC Mbr— порт – член port-channel (LAG). • Probe — порт зондирования.
Admin Mode	Административное состояние порта. Порт должен быть включенным, чтобы получить разрешение на доступ к сети. Может быть включенным (enabled) или отключенным (disabled). По умолчанию - включен.
Physical Mode	Требуемые скорость порта и дуплексный режим. Если выбрана поддержка автосогласования, то дуплексный режим и скорость задаются в процессе автосогласования. Обратите внимание, что анонсируется максимально возможные показатели порта (полный дуплекс, 100M). В противном случае этот объект определяет дуплексный режим порта и скорость передачи. По умолчанию - Auto.
Physical Status	Скорость порта и дуплексный режим.
Link Status	Информация о статусе линка.
Параметр	Значение
Link Trap	Данный объект определяет, отправлять ли trap при изменении состояния линка. По умолчанию - включено.

Параметр	Значение
LACP Mode	Включен ли LACP на данном порте.

ПРИМЕР: Ниже приведен пример вывода команды для всех портов.

```
(Routing) #show port all
```

Intf	Type	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap	LACP Mode	Actor Timeout
0/1		Enable	Auto	100 Full	Up	Enable	Enable	long
0/2		Enable	Auto	100 Full	Up	Enable	Enable	long
0/3		Enable	Auto		Down	Enable	Enable	long
0/4		Enable	Auto	100 Full	Up	Enable	Enable	long
0/5		Enable	Auto	100 Full	Up	Enable	Enable	long
0/6		Enable	Auto	100 Full	Up	Enable	Enable	long
0/7		Enable	Auto	100 Full	Up	Enable	Enable	long
0/8		Enable	Auto	100 Full	Up	Enable	Enable	long
1/1		Enable			Down	Disable	N/A	N/A
1/2		Enable			Down	Disable	N/A	N/A
1/3		Enable			Down	Disable	N/A	N/A
1/4		Enable			Down	Disable	N/A	N/A
1/5		Enable			Down	Disable	N/A	N/A
1/6		Enable			Down	Disable	N/A	N/A

ПРИМЕР: Ниже приведен пример вывода команды для диапазона портов.

```
(Routing) #show port 0/1-1/6
```

Intf	Type	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap	LACP Mode	Actor Timeout
0/1		Enable	Auto	100 Full	Up	Enable	Enable	long
0/2		Enable	Auto	100 Full	Up	Enable	Enable	long
0/3		Enable	Auto		Down	Enable	Enable	long
0/4		Enable	Auto	100 Full	Up	Enable	Enable	long
0/5		Enable	Auto	100 Full	Up	Enable	Enable	long
0/6		Enable	Auto	100 Full	Up	Enable	Enable	long

0/7	Enable	Auto	100 Full	Up	Enable	Enable	long
0/8	Enable	Auto	100 Full	Up	Enable	Enable	long
1/1	Enable			Down	Disable	N/A	N/A
1/2	Enable			Down	Disable	N/A	N/A
1/3	Enable			Down	Disable	N/A	N/A
1/4	Enable			Down	Disable	N/A	N/A
1/5	Enable			Down	Disable	N/A	N/A
1/6	Enable			Down	Disable	N/A	N/A

show port advertise

Используйте эту команду, чтобы отобразить конфигурацию локальных административных объявлений о состоянии канала, объявлений о состоянии локального рабочего канала и объявлений линка-партнера для интерфейса. Она также отображает приоритет установки скорости и дуплексного режима согласно 802.3 Annex 28B.3. Кроме того, она показывает состояние функции автосогласования, конфигурацию Phy Master/Slave Clock и состояние подключения порта.

Если статус линка down, Clock отображается как «No Link», а рядом с Oper Peer Advertisement и Priority Resolution отображается тире. Если автоматическое согласование отключено, не отображаются поля «Admin Local Link Advertisment», «Operational Local Link Advertisment», «Operational Peer Advertisement» и «Priority Resolution».

Если эта команда выполняется без дополнительного параметра **unit/slot/port**, то отображаются состояние автосогласования и объявления локального рабочего линка для всех портов. Объявление линка будет показывать скорость только в том случае, если функция поддерживается обеими сторонами. Если автоматическое согласование отключено, то объявление рабочего линка не отображается.

Формат show port advertise [*unit/slot/port]*

Режим Privileged EXEC

ПРИМЕР: Ниже приведен пример вывода команды без дополнительных параметров:

```
(Switching)#show port advertise 0/1
Port: 0/1
Type: Gigabit - Level
Link State: Down
Auto Negotiation: Enabled
Clock: Auto
                                  1000f  1000h  100f  100h  10f  10h
-----------------------------------------------------------------------
Admin Local Link Advertisement    no     no     yes   no    yes  no
Oper Local Link Advertisement     no     no     yes   no    yes  no
Oper Peer Advertisement           no     no     yes   yes   yes  yes
```

Priority Resolution yes

(Switching)#show port advertise

Port	Type	Neg	Operational Link Advertisement
0/1	Gigabit - Level	Enabled	1000f, 100f, 100h, 10f, 10h
0/2	Gigabit - Level	Enabled	1000f, 100f, 100h, 10f, 10h
0/3	Gigabit - Level	Enabled	1000f, 100f, 100h, 10f, 10h

show port description

Данная команда отображает описания интерфейсов. Для указания интерфейса LAG вместо **unit/slot/port** можно использовать **lag lag-intf-num**, где **lag-intf-num** - номер порта LAG.

Формат show port description *unit/slot/port*

Режим Privileged EX

Термин	Значение
Interface	unit/slot/port
ifIndex	Индекс интерфейса, связанный с портом.
Термин	Значение
Описание	Описание интерфейса, состоящее из букв и цифр, созданное командой “description”.
MAC address	MAC-адрес порта. Формат - 6 двухзначных шестнадцатеричных чисел, разделенных двоеточиями, например 01:23:45:67:89:AB.
Bit Offset Val	Значение бита смещения.

ПРИМЕР: Вывод командной строки для данной команды.

(Switching) #show port description 0/1

Interface 0/1

ifIndex 1

Description

MAC address 00:10:18:82:0C:10

Bit Offset Val 1

7.2. Команды STP (Spanning Tree Protocol)

В этом разделе описаны команды, используемые для настройки протокола STP (Spanning Tree Protocol). STP помогает предотвратить сетевые петли, дублирование сообщений и вызванную этими причинами нестабильность сети.

ПРИМЕЧАНИЕ: По умолчанию STP включен на всех портах и LAG.

ПРИМЕЧАНИЕ: При отключенном STP система не будет перенаправлять сообщения BPDU.

spanning-tree

Данная команда включает STP.

По умолчанию включено

Формат spanning-tree

Режим Global Config

no spanning-tree

Данная команда отключает STP. При отключении конфигурация STP не удаляется и остаётся доступной для редактирования.

Формат no spanning-tree

Режим Global Config

spanning-tree auto-edge

Используйте эту команду, чтобы позволить интерфейсу стать граничным портом, если он не получает BPDU за определенный промежуток времени.

По умолчанию Включено

Формат spanning-tree auto-edge

Режим Interface Config

no spanning-tree auto-edge

Данная команда сбрасывает статус auto-edge порта на значения по умолчанию.

Формат no spanning-tree auto-edge

Режим Interface Config

spanning-tree bpdufilter

Данная команда позволяет включить фильтр BPDU для интерфейса либо диапазона интерфейсов.

По умолчанию отключено

Формат spanning-tree bpdufilter

Режим Interface Config

no spanning-tree bpdufilter

Данная команда позволяет отключить фильтр BPDU для интерфейса либо диапазона интерфейсов.

По умолчанию отключено

Формат spanning-tree bpdufilter

Режим Interface Config

spanning-tree bpdufilter default

Данная команда позволяет включить фильтр BPDU для всех граничных интерфейсов.

По умолчанию отключено

Формат spanning-tree bpdufilter default

Режим Interface Config

no spanning-tree bpdufilter default

Данная команда позволяет отключить фильтр BPDU на всех граничных интерфейсах.

По умолчанию отключено

Формат no spanning-tree bpdufilter default

Режим Interface Config

spanning-tree bpduguard

Используйте эту команду для включения BPDU Guard на коммутаторе.

По умолчанию отключено

Формат spanning-tree bpduguard

Режим Global Config

no spanning-tree bpduguard

Используйте эту команду для отключения BPDU Guard на коммутаторе.

По умолчанию отключено

Формат no spanning-tree bpduguard

Режим Global Config

spanning-tree bpdumigrationcheck

Используйте эту команду для принудительной передачи BPDU RSTP (rapid spanning tree) и MSTP (multiple spanning tree). Укажите параметр **the unit/slot/port** для передачи BPDU из указанного интерфейса или используйте ключевое слово **all** для передачи RST или MST BPDU со всех интерфейсов. Эта команда активирует принудительную передачу BPDU в момент выполнения команды, поэтому она не меняет конфигурацию системы или не имеет «no-» версии.

Формат spanning-tree bpdumigrationcheck {*unit/slot/port* | all}

Режим Global Config

spanning-tree configuration name

Данная команда настраивает идентификатор конфигурации (Configuration Identifier Name). Данный параметр используется для определения конфигурации, которую данный коммутатор использует в настоящее время. **name** – строка длиной до 32 символов.

По умолчанию Основной MAC-адрес в шестнадцатеричном формате

Формат spanning-tree configuration name *name*

Режим Global Config

no spanning-tree configuration name

Эта команда возвращает значение идентификатора конфигурации к настройкам по умолчанию.

Формат no spanning-tree configuration name

Режим Global Config

spanning-tree configuration revision

Данная команда настраивает номер ревизии конфигурации STP (Configuration Identifier Revision level). Данный параметр используется при определения конфигурации, которую данный коммутатор использует в настоящее время. Значение Configuration Identifier Revision Level - число в диапазоне от 0 до 65535.

По умолчанию 0

Формат spanning-tree configuration revision *0-65535*

Режим Global Config

no spanning-tree configuration revision

Данная команда возвращает номер ревизии конфигурации STP к настройкам по умолчанию.

Формат no spanning-tree configuration revision

Режим Global Config

spanning-tree cost

Данная команда настраивает стоимость внешнего пути для порта, используемую экземпляром MST. При использовании ключевого слова **auto** стоимость пути от порта до корневого коммутатора вычисляется автоматически в зависимости от скорости интерфейса. Для настройки параметра вручную настройте значение **cost** в диапазоне 1 – 200000000.

По умолчанию auto

Формат spanning-tree cost {*cost* | auto}

Режим Interface Config

no spanning-tree cost

Данная команда сбрасывает стоимость внешнего пути порта, на настройки по умолчанию.

Формат no spanning-tree cost

Режим Interface Config

spanning-tree edgeport

Эта команда указывает, что интерфейс (или диапазон интерфейсов) является граничным портом в пределах common and internal spanning tree (CIST). Это позволяет этому порту переходить в состояние пересылки без задержки.

Формат spanning-tree edgeport

Режим Interface Config

no spanning-tree edgeport

Эта команда указывает, что порт не является граничным портом в пределах CIST.

Формат no spanning-tree edgeport

Режим Interface Config

spanning-tree forward-time

Данная команда настраивает значение параметра Bridge Forward Delay для CIST. Значение «forward-time» принадлежит диапазону от 4 до 30 секунд, при этом значение больше или равно (Bridge Max Age / 2) + 1.

По умолчанию 15

Формат spanning-tree forward-time *4-30*

Режим Global Config

no spanning-tree forward-time

Данная команда настраивает значение параметра Bridge Forward Delay на установки по умолчанию.

Формат no spanning-tree forward-time

Режим Global Config

spanning-tree max-age

Данная команда настраивает значение параметра Bridge Max Age для CIST. Значение «max-age» принадлежит диапазону от 6 до 40 секунд, при этом значение меньше или равно 2 x (Bridge Forward Delay - 1).

По умолчанию 20

Формат spanning-tree max-age 6-40

Режим Global Config

no spanning-tree max-age

Данная команда сбрасывает параметр Bridge Forward Max на значения по умолчанию.

Формат no spanning-tree max-age

Режим Global Config

spanning-tree max-hops

Данная команда настраивает значение параметра Bridge Max Hops для CIST. Диапазон значений: 6 – 40.

По умолчанию 20

Формат spanning-tree max-hops *6-40*

Режим Global Config

no spanning-tree max-hops

Данная команда сбрасывает параметр Bridge Max Hops на значения по умолчанию.

Формат no spanning-tree max-hops

Режим Global Config

spanning-tree mst

Эта команда устанавливает Path Cost (стоимость пути) или Port Priority (приоритет порта) в экземпляре multiple spanning tree (MST) или в CIST. Необязательный параметр **mstid**, соответствующий существующему экземпляру MST, применяет конфигурацию именно для этого экземпляра MST. Если вы укажете 0 (определенный в качестве CIST ID по умолчанию) в качестве значения **mstid**, конфигурация применяется для экземпляра CIST.

Если вы укажете опцию **cost**, команда установит стоимость пути для этого порта в пределах экземпляра MST или в экземплярах CIST, в зависимости от параметра **mstid**. Диапазон значений «**path cost**»: 1 – 200000000 либо **auto**. При выборе **auto** стоимость пути рассчитывается из скорости соединения.

Если вы укажете опцию **port-priority**, эта команда устанавливает приоритет для этого порта в конкретном экземпляре MST или в экземпляре CIST в зависимости от параметра **mstid**. Значение «**port-priority**» - число в диапазоне от 0 до 240, с шагом 16.

По умолчанию cost—auto

port-priority—128

Формат spanning-tree mst *mstid* {{cost *1-200000000* | auto} | port-priority *0-240*}

Режим Interface Config

no spanning-tree mst

Эта команда сбрасывает Path Cost (стоимость пути) или Port Priority (приоритет порта) в экземпляре MST или CIST на соответствующие значения по умолчанию. Необязательный параметр **mstid**, соответствующий существующему экземпляру MST, применяет конфигурацию для этого экземпляра MST. Если вы укажете 0 (определенный в качестве CIST ID по умолчанию) в качестве значения **mstid**, конфигурация применяется для экземпляра CIST

Если вы укажете опцию **cost**, команда установит стоимость пути для этого порта в пределах экземпляра MST или в экземплярах CIST, в зависимости от параметра **mstid**, на значения по умолчанию, то есть настроит стоимость пути исходя из скорости канала.

Если вы укажете опцию **port-priority**, эта команда устанавливает приоритет для этого порта в конкретном экземпляре MST или в экземпляре CIST в зависимости от параметра **mstid**, на значения по умолчанию.

Формат no spanning-tree mst *mstid* {cost | port-priority}

Режим Interface Config

spanning-tree mst instance

Данная команда добавляет экземпляр MST на коммутатор. Параметр *mstid* – число в диапазоне от 1 до 4094, соответствующий ID добавляемого экземпляра. Максимальное количество экземпляров, поддерживаемое коммутатором – 4.

По умолчанию нет

Формат spanning-tree mst instance *mstid*

Режим Global Config

no spanning-tree mst instance

Эта команда удаляет из коммутатора экземпляр MST и перераспределяет все VLAN, выделенные удаленному экземпляру в CIST. Параметр *mstid* – это число, которое соответствует удаляемому экземпляру MST.

Формат no spanning-tree mst instance *mstid*

Режим Global Config

spanning-tree mst priority

Данная команда устанавливает приоритет моста для конкретного экземпляра MST. Параметр **mstid** – это число, которое соответствует существующему экземпляру MST. Значение приоритета – число в диапазоне от 0 до 4094.

Если вы укажете 0 (определенный в качестве CIST ID по умолчанию) в качестве значения **mstid**, команда установит новый приоритет моста для CIST. Значение приоритета моста – число в диапазоне от 0 до 4094. 12 наименее значимых битов маскируются согласно спецификации 802.1s. Это округляет приоритет вниз до следующего верного приоритета.

По умолчанию 32768

Формат spanning-tree mst priority *mstid 0-4094*

Режим Global Config

no spanning-tree mst priority

Данная команда сбрасывает приоритет моста для конкретного экземпляра MST на значения по умолчанию. Параметр **mstid** – это число, которое соответствует существующему экземпляру MST.

Если вы укажете 0 (определенный в качестве CIST ID по умолчанию) в качестве значения **mstid**, команда установит значения по умолчанию для приоритета моста CIST.

Формат no spanning-tree mst priority *mstid*

Режим Global Config

spanning-tree mst vlan

Эта команда добавляет связь между экземпляром MST и одной или несколькими VLAN таким образом, что VLAN(-ы) перестают быть связанными с CIST. Параметр **mstid** – это идентификатор экземпляра MST в диапазоне от 0 до 4094. Параметр **vlanid** может быть указан как VLAN, а также как список либо диапазон VLAN. Чтобы указать список VLAN, введите список идентификаторов VLAN в диапазоне от 1 до 4093, каждый из которых разделен запятой без пробелов между ними. Чтобы указать диапазон VLAN, укажите начальный и конечный идентификатор VLAN через дефис (-).

Пробелы и нули не допускаются. Идентификатор VLAN может существовать в системе, а может и не существовать.

Формат spanning-tree mst vlan *mstid vlanid*

Режим Global Config

no spanning-tree mst vlan

Эта команда удаляет связь между экземпляром MST и одной или несколькими VLAN таким образом, что VLAN(-ы) снова начинают быть связанными с CIST.

Формат no spanning-tree mst vlan *mstid vlanid*

Режим Global Config

spanning-tree port mode

Данная команда настраивает административное состояние порта таким образом, чтобы он был доступен для использования spanning tree.

По умолчанию включено

Формат spanning-tree port mode

Режим Interface Config

no spanning-tree port mode

Данная команда настраивает административное состояние порта таким образом, чтобы он был не доступен для использования **spanning tree**.

Формат no spanning-tree port mode

Режим Interface Config

spanning-tree port mode all

Данная команда настраивает административное состояние портов коммутатора таким образом, чтобы все порты были доступны для использования **spanning tree**.

По умолчанию включено

Формат spanning-tree port mode all

Режим Global Config

no spanning-tree port mode all

Данная команда настраивает административное состояние портов коммутатора таким образом, чтобы все порты были недоступны для использования spanning tree.

Формат no spanning-tree port mode all

Режим Global Config

spanning-tree tcnguard

Используйте эту команду для включения TCN guard на интерфейсе. Когда эта функция включена, TCN Guard запрещает интерфейсу распространение любой информации об изменении топологии, полученной через этот интерфейс.

По умолчанию Включено

Формат spanning-tree tcnguard

Режим Interface Config

no spanning-tree tcnguard

Данная команда сбрасывает состояние TCN guard на значение по умолчанию.

Формат no spanning-tree tcnguard

Режим Interface Config

spanning-tree transmit

Данная команда настраивает параметр Bridge Transmit Hold Count.

По умолчанию 6

Формат spanning-tree transmit tree hold-count count

Режим Global Config

Параметр	Описание
hold-count	Параметр Bridge Tx hold-count. Диапазон значений: 1 – 10.

show spanning-tree

Данная команда отображает настройки CIST. Показывается следующая информация.

Формат show spanning-tree

Режимы Privileged EXEC

User EXEC

Термин	Значение
Bridge Priority	Приоритет моста для CIST. Диапазон значений: 0 – 61440. Отображается в шестнадцатеричном формате, кратно 4096.

Термин	Значение
Bridge Identifier	Идентификатор моста для CIST. Он составляется с использованием приоритета моста и базового MAC-адреса моста.
Time Since Topology Change	Время в секундах.
Topology Change Count	Количество изменений.
Topology Change in Progress	Бинарное значение, указывающее, выполняется ли в данный момент изменение топологии на любом порту, назначенном для CIST.
Designated Root	Идентификатор корневого моста. Он составляется с использованием приоритета моста и базового MAC-адреса моста.
Root Path Cost	Значение стоимости корневого пути для CIST.
Root Port Identifier	Идентификатор порта для доступа к назначенному корневому мосту для CIST.
Bridge Max Age	Вычисленное значение.
Bridge Max Hops	Счетчик максимального количества прыжков до моста для устройства.
Root Port Bridge	Вычисленное значение.
Forward Delay Hello Time	Настроенное значение параметра для CIST.
Bridge Hold Time	Минимальное время между передачей Configuration Bridge Protocol Data Units (BPDUs).
CST Regional Root	Идентификатор моста регионального корня CIST. Составляется с использованием приоритета моста и базового MAC-адреса моста.
Regional Root Path Cost	Стоимость пути к региональному корню CIST.
Associated FIDs	Список идентификаторов базы переадресации, связанных с этим экземпляром.

Термин	Значение
Associated VLANs	Список VLAN ID, связанных с этим экземпляром.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show spanning-tree
Bridge Priority ..... 32768
Bridge Identifier ..... 80:00:00:10:18:48:FC:07
Time Since Topology Change ..... 8 day 3 hr 22 min 37 sec
Topology Change Count ..... 0
Topology Change in progress..... FALSE
Designated Root..... 80:00:00:10:18:48:FC:07
Root Path Cost..... 0
Root Port Identifier ..... 00:00
Bridge Max Age ..... 20
Bridge Max Hops..... 20
Bridge Tx Hold Count ..... 6
Bridge Forwarding Delay ..... 15
Hello Time..... 2
Bridge Hold Time ..... 6
CST Regional Root..... 80:00:00:10:18:48:FC:07
Regional Root Path Cost..... 0
        Associated FIDs       Associated VLANs
        ---------------       ----------------
```

show spanning-tree brief

Эта команда отображает настройки **spanning-tree** для моста. Отображается следующая информация.

Формат show spanning-tree brief

Режимы Privileged EXEC

User EXEC

Термин	Значение
Bridge Priority	Заданное значение.
Bridge Identifier	Идентификатор моста выбранного экземпляра MST. Он составляется с использованием приоритета моста и базового MAC-адреса моста.

Термин	Значение
Bridge Max Age	Заданное значение.
Bridge Max Hops	Счетчик максимального количества прыжков до моста для устройства.
Bridge Hello Time	Заданное значение.
Bridge Forward Delay	Заданное значение.
Bridge Hold Time	Минимальное время между передачей Configuration Bridge Protocol Data Units (BPDUs).

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show spanning-tree brief
Bridge Priority .....32768
Bridge Identifier .....80:00:00:10:18:48:FC:07
Bridge Max Age .....20
Bridge Max Hops.....20
Bridge Hello Time.....2
Bridge Forward Delay.....15
Bridge Hold Time .....6
(Routing) #
```

show spanning-tree interface

Эта команда отображает настройки и параметры для конкретного порта коммутатора в пределах CIST. Параметр **unit/slot/port** – нужный порт коммутатора. Для указания интерфейса LAG вместо **unit/slot/port** можно использовать lag **lag-intf-num**. Также для определения интефейса LAG можно использовать lag **lag-intf-num**, где **lag-intf-num** - номер порта LAG. При выполнении команды отображаются следующие данные.

Формат show spanning-tree interface *unit/slot/port*|lag *lag-intf-num*

Режимы Privileged EXEC

User EXEC

Термин	Значение
Hello Time	Период "hello" для данного порта.
Port Mode	Включен или выключен.

Термин	Значение
BPDU Guard Effect	Включен или выключен.
TCN Guard	Включено или выключено распространение информации об изменении топологии на другие порты.
Auto Edge	Включена или выключена функция, заставляющая порт, не получавший BPDU на протяжении периода edge delay , становиться граничным портом и перейти на режим пересылки быстрее.
Port Up Time Since Counters Last Cleared	Время, прошедшее со сброса счетчиков порта, в днях, часах, минутах и секундах.
STP BPDUs Transmitted	Отправлено STP BPDU.
STP BPDUs Received	Принято STP BPDU.
RSTP BPDUs Transmitted	Отправлено RSTP BPDU.
STP BPDUs Received	Принято RSTP BPDU.
MSTP BPDUs Transmitted	Отправлено MSTP BPDU.
MSTP BPDUs Received	Принято STP BPDU.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) >show spanning-tree interface 0/1
Hello Time..... Not Configured
Port Mode ..... Enabled
BPDU Guard Effect..... Disabled
Root Guard ..... FALSE
Loop Guard..... FALSE
TCN Guard ..... FALSE
BPDU Filter Mode ..... Disabled
BPDU Flood Mode..... Disabled
Auto Edge ..... TRUE
```

Port Up Time Since Counters Last Cleared..... 8 day 3 hr 39 min 58 sec
STP BPDUs Transmitted..... 0
STP BPDUs Received..... 0
RSTP BPDUs Transmitted..... 0
RSTP BPDUs Received..... 0
MSTP BPDUs Transmitted..... 0
MSTP BPDUs Received..... 0
(Routing) >

ПРИМЕР: Вывод командной строки для данной команды.

(Routing) >show spanning-tree interface lag 1
Hello Time..... Not Configured
Port Mode..... Enabled
BPDU Guard Effect..... Disabled
Root Guard..... FALSE
Loop Guard..... FALSE
TCN Guard..... FALSE
BPDU Filter Mode..... Disabled
BPDU Flood Mode..... Disabled
Auto Edge..... TRUE
Port Up Time Since Counters Last Cleared..... 8 day 3 hr 42 min 5 sec
STP BPDUs Transmitted..... 0
STP BPDUs Received..... 0
RSTP BPDUs Transmitted..... 0
RSTP BPDUs Received..... 0
MSTP BPDUs Transmitted..... 0
MSTP BPDUs Received..... 0
(Routing) >

show spanning-tree mst detailed

Эта команда детально отображает параметры настроек длля экземпляра MST.

Формат show spanning-tree mst detailed *mstid*

Режим Privileged EXEC
User EXEC

Параметр	Описание
mstid	Идентификатор экземпляра MST. Диапазон значений: 0 – 4094.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) >show spanning-tree mst detailed 0
MST Instance ID..... 0
MST Bridge Priority..... 32768
MST Bridge Identifier ..... 80:00:00:10:18:48:FC:07
Time Since Topology Change ..... 8 day 3 hr 47 min 7 sec
Topology Change Count ..... 0
Topology Change in progress..... FALSE
Designated Root..... 80:00:00:10:18:48:FC:07
Root Path Cost..... 0
Root Port Identifier ..... 00:00
        Associated FIDs      Associated VLANs
        ---------------      ----------------
(Routing) >
```

show spanning-tree mst port detailed

Эта команда отображает настройки и параметры для конкретного порта коммутатора в пределах конкретного экземпляра MST. Параметр **mstid** – это число, которое соответствует существующему экземпляру MST. Параметр **unit/slot/port** – нужный порт коммутатора. Для указания интерфейса LAG вместо **unit/slot/port** можно использовать **lagintf-num**. Также для определения интефейса LAG можно использовать lag **lag-intf-num**, **где lag-intf-num** - номер порта LAG.

Формат show spanning-tree mst port detailed *mstid unit/slot/port*|lag *lag-intf-num*

Режимы Privileged EXEC

User EXEC

Термин	Значение
MST Instance ID	Идентификатор существующего экземпляра MST. Диапазон значений: 0 – 4094.
Port Identifier	Идентификатор конкретного порта в пределах выбранного экземпляра MST. Он составляется с использованием приоритета и номера интерфейса порта.
Port Priority	Приоритет для конкретного порта в пределах выбранного экземпляра MST. Кратно 16.
Port Forwarding State	Текущее состояние spanning tree на данном порте.

Термин	Значение
Port Role	Каждый активный порт моста MST получает роль порта для каждого spanning tree. Роль порта может быть: Корневой (Root Port), Назначенный (Designated Port), Альтернативный (Alternate Port), Резервный (Backup Port), Мастер (Master Port) либо Отключенный (Disabled Port)
Auto-Calculate Port Path Cost	Включено ли автоматическое вычисление стоимости пути для порта.
Port Path Cost	Настроенное значение параметра внутренней стоимости пути порта.
Designated Root	Идентификатор назначенного корня для данного порта.
Root Path Cost	Стоимость пути к корневому мосту для данного экземпляра. Равняется нулю, если мост - корневой мост этого экземпляра.
Designated Bridge	Идентификатор моста с назначенным портом (Designated Port).
Designated Port Identifier	Порт на назначенном мосту (Designated Bridge), предлагающий самую низкую стоимость пути к LAN.

Если вы укажете 0 (определенный в качестве CIST ID по умолчанию) в качестве значения **mstid**, команда отобразит настройки и параметры для определенного порта коммутатора в пределах CIST. Параметр **unit/slot/port** – нужный порт коммутатора. В данном случае отображается следующее:

Термин	Значение
Port Identifier	Идентификатор порта для конкретного порта в пределах CIST.
Port Priority	Приоритет данного порта в пределах CIST.
Port Identifier	Идентификатор порта для конкретного порта в пределах CIST.
Port Priority	Приоритет данного порта в пределах CIST.
Термин	Значение
Port Forwarding State	Состояние передачи данного порта в пределах CIST.
Port Role	Приоритет данного interface в пределах CIST.

Термин	Значение
Auto-Calculate Port Path Cost	Включено ли автоматическое вычисление стоимости пути для порта.
Port Path Cost	Настроенная стоимость пути для указанного интерфейса.
Auto-Calculate External Port Path Cost	Включено ли автоматическое вычисление стоимости пути для внешнего порта.
External Port Path Cost	Стоимость пути до корневого моста CIST через границу области. Это означает, что если порт является граничным портом для области MSTP, то используется стоимость внешнего пути.
Designated Root	Идентификатор заданного корня для данного порта в пределах CIST.
Root Path Cost	Стоимость корневого пути к LAN при помощи данного порта.
Designated Bridge	Мост, содержащий назначенный порт (Designated Port).
Designated Port Identifier	Порт на назначенном мосту (Designated Bridge), предлагающий самую низкую стоимость пути к LAN.
Topology Change Acknowledgement	Значение флага в следующей передаче данных Configuration Bridge Protocol Data Unit (BPDU), указывающее, что для этого порта выполняется изменение топологии.
Hello Time	Период "hello" для данного порта.
Edge Port	Настроенное значение, указывающее, этот порт является граничным.
Edge Port Status	Вычисленное значение состояния граничного порта. True – рабочий граничный порт; false – любой другой случай.
Point To Point MAC Status	Вычисленное значение, указывающее, что этот порт является частью линка «точка-точка».
CST Regional Root	Региональный корневой идентификатор (regional root identifier), используемый для данного порта.
CST Internal	Внуреннаяя стоимость корневого пути к LAN при помощи назначенного внешнего порта.

Root Path Cost

ПРИМЕР: Выполнение команды в формате slot/port.

```
(Routing) >show spanning-tree mst port detailed 0 0/1
Port Identifier.....80:01
Port Priority.....128
Port Forwarding State.....Disabled
Port Role.....Disabled
Auto-calculate Port Path Cost.....Enabled
Port Path Cost.....0
Auto-Calculate External Port Path Cost.....Enabled
External Port Path Cost.....0
Designated Root.....80:00:00:10:18:48:FC:07
Root Path Cost.....0
Designated Bridge.....80:00:00:10:18:48:FC:07
Designated Port Identifier.....00:00
Topology Change Acknowledge.....FALSE
Hello Time.....2
Edge Port.....FALSE
Edge Port Status.....FALSE
Point to Point MAC Status.....TRUE
CST Regional Root.....80:00:00:10:18:48:FC:07
CST Internal Root Path Cost.....0
Loop Inconsistent State.....FALSE
Transitions Into Loop Inconsistent State.....0
Transitions Out Of Loop Inconsistent State.....0
```

ПРИМЕР: Вывод команды с использованием номера интерфейса LAG.

```
(Routing) >show spanning-tree mst port detailed 0 lag 1
Port Identifier.....60:42
Port Priority.....96
Port Forwarding State.....Disabled
Port Role.....Disabled
Auto-calculate Port Path Cost.....Enabled
Port Path Cost.....0
Auto-Calculate External Port Path Cost.....Enabled
External Port Path Cost.....0
Designated Root.....80:00:00:10:18:48:FC:07
Root Path Cost.....0
```

```
Designated Bridge.....80:00:00:10:18:48:FC:07
Designated Port Identifier.....00:00
Topology Change Acknowledge.....FALSE
Hello Time.....2
Edge Port.....FALSE
Edge Port Status.....FALSE
Point to Point MAC Status.....TRUE
CST Regional Root.....80:00:00:10:18:48:FC:07
CST Internal Root Path Cost .....0
Loop Inconsistent State.....FALSE
Transitions Into Loop Inconsistent State.....0
Transitions Out Of Loop Inconsistent State .....0
--More-- or (q)uit
(Routing) >
```

show spanning-tree mst port summary

Эта команда отображает настройки одного или всех портов в пределах указанного экземпляра MST. Параметр **mstid** – идентификатор конкретного экзепляра MST. Параметр **{unit/slot/port|all}** – нужный порт коммутатора (либо все порты). Для указания интерфейса LAG вместо **unit/slot/port** можно использовать **lag-intf-num**. Также для определения интефейса LAG можно использовать lag **lag-intf-num**, где **lag-intfnum** - номер порта LAG.

Если вы укажете 0 (определенный в качестве CIST ID по умолчанию) в качестве значения **mstid**, сводная информация о состоянии будет отображаться для одного или для всех портов коммутатора в пределах CIST.

Формат show spanning-tree mst port summary *mstid* {*unit/slot/port* |lag *lag-intf-num*| all}

Режимы Privileged EXEC

User EXEC

Термин	Значение
MST Instance ID	Экземпляр MST, связанный с данным портом.
Interface	unit/slot/port
STP Mode	Указывает на то, включена или выключена функция spanning tree на этом порте.
Type	В данный момент не используется.
STP State	Состояние передачи на порту в указанных экземплярах spanning tree.

Термин	Значение
Port Role	Роль данного порта в пределах spanning tree.
Desc	Указывает, находится ли порт в несогласованном состоянии цикла или нет. Это поле пустое, если функция loop guard недоступна.

ПРИМЕР: Выполнение команды в формате slot/port.

```
(Routing) >show spanning-tree mst port summary 0 0/1
MST Instance ID       CST
 Interface            STP Mode    Type        STP State              Port Role    Desc
 ---------------------------------------------------------------------------------
 0/1                  Enabled                 Disabled               Disabled
```

ПРИМЕР: Вывод команды с использованием номера интерфейса LAG.

```
(Routing) >show spanning-tree mst port summary 0 lag 1
MST Instance ID       CST
 Interface            STP Mode    Type        STP State              Port Role    Desc
 ---------------------------------------------------------------------------------
 3/1                  Enabled                 Disabled               Disabled
```

show spanning-tree mst port summary active

Эта команда отображает настройки для портов в указанном экземпляре MST, которые находятся в активном состоянии.

Формат Show spanning-tree mst port summary *mstid active*

Режимы Privileged EXEC

User EXEC

Термин	Значение
MST Instance ID	Идентификатор существующего экземпляра MST.
Interface	unit/slot/port
STP Mode	Указывает на то, включена или выключена функция spanning tree на этом порте.
Type	В данный момент не используется.

Термин	Значение
STP State	Состояние передачи на порту в указанных экземплярах spanning tree.
Port Role	Приоритет данного порта в пределах spanning tree.
Desc	Указывает, находится ли порт в несогласованном состоянии цикла или нет. Это поле пустое, если функция loop guard не включена.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) >show spanning-tree mst port summary 0 active

Interface          STP Mode  Type      STP State          Port Role  Desc
-------------------------------------------------------------------------------
```

show spanning-tree mst summary

Данная команда отображает сводную информацию обо всех экземплярах MST на коммутаторе. Показывается следующая информация.

Формат show spanning-tree mst summary

Режимы Privileged EXEC

User EXEC

Термин	Значение
MST Instance ID List	Список идентификаторов MST, настроенных к настоящему времени. Для каждого MSTID: • Список индентификаторов базы передачи, связанных с этим экземпляром. • Список VLAN ID, связанных с этим экземпляром. • Связанные VLAN.

show spanning-tree summary

Эта команда отображает настройки и параметры spanning-tree для коммутатора. При выполнении команды отображаются следующие данные.

Формат show spanning-tree summary

Режимы Privileged EXEC

User EXEC

Термин	Значение
Spanning Tree Adminmode	Включено или выключено.
Spanning Tree Version	Версия 802.1, поддерживаемая в настоящий момент (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d), основанная на параметре Force Protocol Version.
BPDU Guard Mode	Включено или выключено.
BPDU Filter Mode	Включено или выключено.
Configuration Name	Идентификатор конфигурации, используемой в данный момент.
Configuration Revision Level	Идентификатор ревизии конфигурации, используемой в данный момент.
Configuration Digest Key	Сгенерированный ключ, используемый при обмене BPDU.
Configuration Format Selector	Указывает версию конфигурационного формата, используемую при обмене BPDU. Значение по умолчанию - 0.
MST Instances	Список экземпляров MST, настроенных на коммутаторе.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) >show spanning-tree summary
Spanning Tree Adminmode ..... Enabled
Spanning Tree Version ..... IEEE 802.1s
BPDU Guard Mode..... Disabled
BPDU Filter Mode ..... Disabled
Configuration Name ..... ****
Configuration Revision Level..... ****
Configuration Digest Key..... ****
Configuration Format Selector ..... 0
No MST instances to display.
```

*в выводе вместо символов * будут данные, заданные при настройке

7.3. Команды VLAN

В этом разделе описаны команды, которые используются для настройки VLAN.

vlan database

Данная команда предоставляет доступ к режиму VLAN config, который позволяет вам настроить характеристики VLAN

Формат vlan database

Режим Privileged EXEC

network mgmt_vlan

Данная команда настраивает VLAN ID сети управления.

По умолчанию 1

Формат network mgmt_vlan 1-4093

Режим Privileged EXEC

no network mgmt_vlan

Данная команда сбрасывает настройки VLAN ID сети управления на значения по умолчанию.

Формат no network mgmt_vlan

Режим Privileged EXEC

vlan

Данная команда создаёт новую VLAN и назначает ID. ID – идентификатор VLAN (ID 1 зарезервирован для VLAN по умолчанию). Диапазон: 2 – 4093.

Формат vlan *2-4093*

Режим VLAN Config

no vlan

Данная команда удаляет существующую сеть VLAN. ID – идентификатор VLAN (ID 1 зарезервирован для VLAN по умолчанию). Диапазон: 2 – 4093.

Формат no vlan *2-4093*

Режим VLAN Config

vlan acceptframe

Данная команда устанавливает режим получения фреймов на интерфейсе или диапазоне интерфейсов. В режиме «VLAN Only» отбрасываются нетегированные фреймы либо фреймы с приоритетом, полученные на этом интерфейсе. В режиме «Admit All» нетегированные фреймы либо фреймы с приоритетом, полученные на этом интерфейсе, принимаются, и им присваивается значение VLAN ID интерфейса для данного порта. В режиме «admituntaggedonly» на интерфейсе принимаются только нетегированные фреймы, тегированные фреймы отбрасываются. В любом случае, тегированные фреймы VLAN перенаправляются в соответствии со спецификацией IEEE 802.1Q VLAN.

По умолчанию All

Формат vlan acceptframe {admituntaggedonly | vlanonly | all}

Режим Interface Config

no vlan acceptframe

Данная команда сбрасывает режим получения фреймов на интерфейсе или диапазоне интерфейсов на значения по умолчанию.

Формат no vlan acceptframe

Режим Interface Config

vlan ingressfilter

Эта команда активирует входную фильтрацию на интерфейсе или в диапазоне интерфейсов. Если входная фильтрация отключена, то фреймы, полученные с идентификаторами VLAN, не соответствующими членству VLAN принимающего интерфейса, принимаются и перенаправляются в порты, входящие в эту VLAN.

По умолчанию отключено

Формат vlan ingressfilter

Режим Interface Config

no vlan ingressfilter

Данная команда отключает входную фильтрацию. Если входная фильтрация отключена, то фреймы, полученные с идентификаторами VLAN, не соответствующими членству VLAN принимающего интерфейса, принимаются и перенаправляются в порты, входящие в эту VLAN.

Формат no vlan ingressfilter

Режим Interface Config

vlan internal allocation

Используйте эту команду, чтобы настроить, какие VLAN ID используются для интерфейсов маршрутизации на основе портов. Когда создается интерфейс маршрутизации на основе порта, неиспользуемые VLAN ID назначаются внутренне этим интерфейсам.

Формат vlan internal allocation {base *vlan-id* | policy ascending | policy decending}

Режим Global Config

Параметр	Описание
base vlan-id	Первый VLAN ID, который должен быть назначен интерфейсу маршрутизации на основе портов.

Параметр	Описание
policy ascending	Задается политика назначения VLAN ID интерфейсам маршрутизации на основе портов, начиная с base vlan-id в сторону увеличения ID.
policy descending	Задается политика назначения VLAN ID интерфейсам маршрутизации на основе портов, начиная с base vlan-id в сторону уменьшения ID.

vlan makestatic

Эта команда изменяет динамически создаваемую VLAN (созданную GVRP) на статическую VLAN (то есть ту, которая постоянно настроена и определена). ID – идентификационный номер VLAN. Диапазон: 2 – 4093.

Формат vlan makestatic 2-4093

Режим VLAN Config

vlan name

Данная команда изменяет имя сети VLAN. Имя – строка из цифр и букв (до 32 символов), а ID – идентификационный номер VLAN. Диапазон: 1 – 4093.

По умолчанию ID VLAN по умолчанию – 1

Прочие VLAN - пустая строка

Формат vlan name 1-4093 name

Режим VLAN Config

no vlan name

Данная команда изменяет имя сети VLAN на пустую строку.

Формат no vlan name 1-4093

Режим VLAN Config

vlan participation

Эта команда настраивает степень участия для определенного интерфейса или диапазона интерфейсов в VLAN. ID – идентификационный номер VLAN, а «interface» – действительный номер интерфейса.

Формат vlan participation {exclude | include | auto} *1-4093*

Режим Interface Config

Опции участия:

Опция	Значение
include	Интерфейс всегда является членом данной VLAN. Это эквивалентно «registration fixed».
exclude	Интерфейс никогда не является членом данной VLAN. Это эквивалентно «registration forbidden».
auto	Интерфейс динамически регистрируется в этой VLAN с помощью GVRP и не будет участвовать в этой VLAN, если на этом интерфейсе не будет получен запрос соединения. Это эквивалентно «registration normal».

vlan participation all

Эта команда настраивает степень участия для всех интерфейсов в VLAN. ID – идентификационный номер VLAN.

Формат vlan participation all {exclude | include | auto} 1-4093

Режим Global Config

Опции участия:

Опции участия	Значение
include	Интерфейс всегда является членом данной VLAN. Это эквивалентно «registration fixed».
exclude	Интерфейс никогда не является членом данной VLAN. Это эквивалентно «registration forbidden».
auto	Интерфейс динамически регистрируется в этой VLAN с помощью GVRP. Интерфейс не будет участвовать в этой VLAN, если на этом интерфейсе не будет получен запрос соединения. Это эквивалентно «registration normal».

vlan port acceptframe all

Данная команда устанавливает режим получения фреймов на всех интерфейсах.

По умолчанию All

Формат vlan port acceptframe all {vlanonly | admituntaggedonly |all}

Режим Global Config

Возможные режимы:

Режим	Значение
VLAN Only mode	Нетегированные либо фреймы с приоритетом, полученные на этом интерфейсе, отбрасываются.
Admit Untagged Only mode	Тегированные либо тегированные фреймы с приоритетом, полученные на этом интерфейсе, отбрасываются.
Admit All mode	Нетегированные либо фреймы с приоритетом, полученные на этом интерфейсе, принимаются, и им присваивается значение VLAN ID интерфейса для данного порта.

В любом случае, тегированные фреймы VLAN перенаправляются в соответствии со спецификацией IEEE 802.1Q VLAN.

no vlan port acceptframe all

Данная команда устанавливает режим получения фреймов «Admit All» на всех интерфейсах. В режиме «Admit All» нетегированные либо фреймы с приоритетом, полученные на этом интерфейсе, принимаются, и им присваивается значение VLAN ID интерфейса для данного порта. В любом случае, тегированные фреймы VLAN перенаправляются в соответствии со спецификацией IEEE 802.1Q VLAN.

Формат no vlan port acceptframe all

Режим Global Config

vlan port ingressfilter all

Данная команда активирует входную фильтрацию на всех портах. Если входная фильтрация отключена, то фреймы, полученные с идентификаторами VLAN, не соответствующими членству VLAN в принимающем интерфейсе, принимаются и перенаправляются в порты, входящие в эту VLAN.

По умолчанию отключено

Формат vlan port ingressfilter all

Режим Global Config

no vlan port ingressfilter all

Данная команда отключает входную фильтрацию на всех портах. Если входная фильтрация отключена, то фреймы, полученные с идентификаторами VLAN, не соответствующими членству VLAN в принимающем интерфейсе, принимаются и перенаправляются в порты, входящие в эту VLAN.

Формат no vlan port ingressfilter all

Режим Global Config

vlan port pvid all

Эта команда изменяет VLAN ID для всех интерфейсов.

По умолчанию 1

Формат vlan port pvid all *1-4093*

Режим Global Config

no vlan port pvid all

Эта команда изменяет VLAN ID для всех интерфейсов на 1.

Формат no vlan port pvid all

Режим Global Config

vlan port tagging all

Эта команда включает тегирование для всех интерфейсов в VLAN. Если тегирование включено, трафик передаётся в виде тегированных фреймов. Если оно отключено, трафик передаётся в виде нетегированных фреймов. ID – идентификационный номер VLAN.

Формат vlan port tagging all *1-4093*

Режим Global Config

no vlan port tagging all

Эта команда отключает тегирование для всех интерфейсов в VLAN. Если оно отключено, трафик передаётся в виде нетегированных фреймов. ID – идентификационный номер VLAN.

Формат no vlan port tagging all

Режим Global Config

vlan pvid

Данная команда меняет VLAN ID на интерфейсе или диапазоне интерфейсов.

По умолчанию 1

Формат vlan pvid *1-4093*

Режим Interface Config

Interface Range Config

no vlan pvid

Данная команда сбрасывает VLAN ID на интерфейсе или диапазоне интерфейсов на 1.

Формат no vlan pvid

Режим Interface Config

vlan tagging

Эта команда включает тегирование для определенного интерфейса или диапазона интерфейсов в VLAN. Если тегирование включено, трафик передаётся в виде

тегированных фреймов. Если оно отключено, трафик передаётся в виде нетегированных фреймов. ID – идентификационный номер VLAN.

Формат vlan tagging *1-4093*

Режим Interface Config

no vlan tagging

Эта команда отключает тегирование для определенного интерфейса или диапазона интерфейсов в VLAN. Если оно отключено, трафик передаётся в виде нетегированных фреймов. ID – идентификационный номер VLAN.

Формат no vlan tagging *1-4093*

Режим Interface Config

remote-span

Данная команда идентифицирует VLAN как RSPAN VLAN.

По умолчанию Нет

Формат remote-span

Режим VLAN configuration

no remote-span

Данная команда удаляет из VLAN информацию RSPAN.

Формат no remote-span

Режим VLAN configuration

show vlan

Эта команда отображает информацию о настроенных частных VLAN, включая первичные и вторичные идентификаторы VLAN, тип (community, isolated или primary) и порты, принадлежащие частной VLAN.

Формат show vlan {vlanid|private-vlan [type]}

Режим Privileged EXEC

User EXEC

Термин	Значение
Primary	Первичный идентификатор VLAN. Диапазон VLAN ID - от 1 до 4093.
Secondary	Вторичный идентификатор VLAN.
Type	Вторичный тип VLAN (community, isolated или primary).
Ports	Порты, ассоциированные с частной VLAN.

Термин	Значение
VLAN ID	Идентификатор VLAN (VID), ассоциированный с каждой VLAN. Диапазон VLAN ID - от 1 до 4093.
VLAN Name	Строка, ассоциированная с данной VLAN для удобства. Она может быть до 32 символов в длину, и состоять из букв, цифр и пробелов. По умолчанию - пустой текст. VLAN ID 1 всегда имеет имя Default. Данное поле не обязательно для использования.
VLAN Type	Тип VLAN. Может быть: Default (VLAN ID = 1), static (настроенная и постоянно определенная VLAN) либо Dynamic. Динамическая VLAN может быть создана путем регистрации GVRP или во время процесса аутентификации 802.1X (DOT1X), если на коммутаторе не существует VLAN с RADIUS-определением.
Interface	unit/slot/port. Параметры для всех портов можно задать с помощью выбираемых параметров в команде.
Current	Степень участия этого порта в данной VLAN. Возможные значения: • Include - Порт всегда является членом данной VLAN. Эквивалентно «registration fixed» в стандарте IEEE 802.1Q. • Exclude - Порт никогда не является членом данной VLAN. Эквивалентно «registration forbidden» в стандарте IEEE 802.1Q. • Autodetect - Порт может быть динамически зарегистрирован в данной VLAN при помощи GVRP. Порт не будет участвовать в этой VLAN, если на этом порте не будет получен запрос соединения. Эквивалентно «registration normal» в стандарте IEEE 802.1Q.
Configured	Настроенная степень участия этого порта в данной VLAN. Возможные значения: • Include - Порт всегда является членом данной VLAN. Эквивалентно «registration fixed» в стандарте IEEE 802.1Q. • Exclude - Порт никогда не является членом данной VLAN. Эквивалентно «registration forbidden» в стандарте IEEE 802.1Q. • Autodetect - Порт может быть динамически зарегистрирован в данной VLAN при помощи GVRP. Порт не будет участвовать в этой VLAN, если на этом порте не будет получен запрос соединения. Эквивалентно «registration normal» в стандарте IEEE 802.1Q.

Термин	Значение
Tagging	Настройки тегирования для этого порта в данной сети VLAN. • Tagged - Передача трафика по этой сети VLAN в виде тегированных фреймов. • Untagged - Передача трафика по этой сети VLAN в виде нетегированных фреймов.

show vlan internal usage

Данная команда отображает информацию о выделении VLAN ID на коммутаторе.

Формат show vlan internal usage

Режимы Privileged EXEC

User EXEC

Термин	Значение
Base VLAN ID	Базовый идентификатор VLAN для внутреннего выделения VLAN на интерфейсе маршрутизации.
Allocation policy	Определяет, выдает ли система идентификаторы VLAN в порядке возрастания или убывания.

show vlan brief

Данная команда выводит список настроенных VLAN.

Формат show vlan brief

Режим Privileged EXEC

User EXEC

Термин	Значение
VLAN ID	Идентификатор VLAN (VID), ассоциированный с каждой VLAN. Диапазон VLAN ID - от 1 до 4093.
VLAN Name	Строка, ассоциированная с данной VLAN для удобства. Она может быть до 32 символов в длину, и состоять из букв, цифр и пробелов. По умолчанию - пустой текст. VLAN ID 1 всегда имеет имя Default. Данное поле не обязательно для использования.
VLAN Type	Тип VLAN. Может быть: Default (VLAN ID = 1), static (настроенная и постоянно определенная VLAN) либо Dynamic (созданная регистрацией GVRP).

show vlan port

Данная команда предоставляет информацию о порте VLAN.

Формат show vlan port {*unit/slot/port* | all}

Режим Privileged EXEC

User EXEC

Термин	Значение
Interface	**unit/slot/port** Параметры для всех портов можно задать с помощью выбираемых параметров в команде.
Port VLAN ID Configured	VLAN ID, который данный порт назначит полученным нетегированным либо тегированным фреймам с приоритетом. Значение должно соответствовать существующей сети VLAN. Значение по умолчанию - 1.
Port VLAN ID Current	Текущий VLAN ID, который данный порт назначит полученным нетегированным либо тегированным фреймам с приоритетом. Значение по умолчанию - 1.
Acceptable Frame Types	Тип фреймов, которые могут быть получены на данном порте. Возможные варианты: 'VLAN only' и 'Admit All'. Если выбрть опцию 'VLAN only', немаркированные либо тегированные фреймы с приоритетом, полученные на этом порте, отбрасываются. Если выбрть опцию 'Admit All', нетегированные либо фреймы с приоритетом, полученные на этом порте, принимаются, и им присваивается значение Port VLAN ID для данного порта. В любом случае, тегированные фреймы VLAN перенаправляются в соответствии со спецификацией 802.1Q VLAN.
Ingress Filtering Configured	Может быть включено либо выключено. Если опция включена - фрейм отбрасывается, если порт не является членом VLAN, с которым этот фрейм ассоциирован. В случае с тегированными фреймами, VLAN определяется по VLAN ID в теге. В случае с нетегированными фреймами, VLAN - это Port VLAN ID, определяемый по порту, получившему данный фрейм. При отключении все фреймы перенаправляются согласно спецификации 802.1Q VLAN. По умолчанию - выключено.
Ingress Filtering Current	Текущая конфигурация входной фильтрации
GVRP	Может быть включен или отключен.

Термин	Значение
Default Priority	Приоритет 802.1p, назначенный для тегированных пакетов, поступающих на порт.
Protected Port	Указывает, является ли данный порт защищенным. «False» - не является, «true» - является.
Switchport mode	Текущий режим switchport для порта.
Operating parameters	Рабочие параметры порта, включающие имя VLAN, правило egress и тип.
Static configuration	Статическая конфигурация порта, включающая имя VLAN, правило egress и тип.
Forbidden VLANs	Конфигурация запрещенных VLAN на порту, включающая VLAN и имя.

7.4. Команды частных VLAN

В этом разделе описаны команды, которые используются для настройки частных VLAN. Частные VLAN обеспечивают изоляцию 2 уровня OSI между портами, которые используют один и тот же широковещательный домен. Другими словами, он позволяет разделять широковещательный домен VLAN на меньшие субдомены «точка-многоточка». Порты, участвующие в частной VLAN, могут быть расположены на любом участке сети уровня 2.

switchport private-vlan

Эта команда определяет ассоциацию частной VLAN для изолированного порта или общего порта, либо преобразование для смешанного порта.

Формат switchport private-vlan {host-association primary-vlan-id secondary-vlan-id | mapping primary-vlan-id {add | remove} secondary-vlan-list}

Режим Interface Config

Параметр	Описание
host-association	Определяет ассоциацию VLAN для общих портов или хоста.
mapping	Определяет преобразование частной VLAN смешанного порта.
primary-vlan-id	Первичный VLAN ID частной VLAN.
secondary-vlan- id	Вторичный (изолированный либо общий) VLAN ID частной VLAN.

Параметр	Описание
add	Ассоциирует вторичную VLAN с первичной.
remove	Удаляет ассоциирование вторичной и первичной VLAN.
secondary-vlan-list	Список вторичных VLAN для преобразования в первичные VLAN.

no switchport private-vlan

Данная команда удаляет ассоциацию или преобразование частной VLAN из порта.

Формат no switchport private-vlan {host-association|mapping}

Режим Interface Config

switchport mode private-vlan

Данная команда настраивает порт как смешанный либо как порт хоста частной сети VLAN. Обратите внимание на то, что свойства каждого режима можно настроить, даже если коммутатор не находится в этом режиме в данный момент. Тем не менее, настройки вступят в силу только тогда, когда коммутатор перейдёт в соответствующий режим.

По умолчанию general

Формат switchport mode private-vlan {host|promiscuous}

Режим Interface Config

Параметр	Описание
host	Настраивает интерфейс как хост-порт частной VLAN. Он может быть изолированным портом или общим портом, в зависимости от вторичной VLAN, с которой он связан.
promiscuous	Настраивает интерфейс как смешанный порт частной VLAN. Смешанный порты - это члены первичной сети VLAN.

no switchport mode private-vlan

Данная команда удаляет ассоциацию или преобразование частной VLAN из порта.

Формат no switchport mode private-vlan

Режим Interface Config

private-vlan

Данная команда настраивает частные VLAN, а также ассоциации между первичными и вторичными VLAN

Формат private-vlan {association [add|remove] secondary-vlanlist|community|isolated|primary}

Режим VLAN Config

Параметр	Описание
association	Ассоциирует первичную и вторичную VLAN.
secondary-vlan-list	Список вторичных VLAN для преобразования в первичные VLAN.
community	Назначает VLAN общей VLAN.
isolated	Назначает VLAN изолированной VLAN.
primary	Назначает VLAN первичной VLAN.

no private-vlan

Эта команда восстанавливает нормальную конфигурацию VLAN.

Формат no private-vlan {association}

Режим VLAN Config

7.5. Порты коммутатора

В этом разделе описываются команды настройки режимов портов коммутатора.

switchport mode

Данная команда позволяет настроить режим порта коммутатора: access (порт доступа), trunk (магистральный порт) или hybrid (гибридный порт).

В режиме Trunk порт становится членом всех VLAN на коммутаторе, кроме тех случаев, когда указан список разрешенных, командой **switchport trunk allowed vlan**. PVID порта устанавливается в Native VLAN, согласно команде **switchport trunk native vlan**. Это означает, что trunk-порты принимают как тегированные, так и нетегированные пакеты. Нетегированные отправляются в Native VLAN, а тегированные пакеты обрабатываются согласно VLAN ID, содержащемуся в пакете. Функция изучения MAC-адреса работает как для тегированных, так и для нетегированных пакетов. Если тегированный пакет получен с идентификатором VLAN, членом которого порт не является, то данный пакет отбрасывается и запоминания MAC-адреса не происходит. Порты Trunk всегда передают пакеты без тегов в native VLAN.

Порт в режиме Access становится членом только одной VLAN. Порт отправляет и получает нетегированный траффик. Он также может получать тегированный трафик. На порте включена входная фильтрация. Если VLAN ID принятого пакета не совпадает с Access VLAN ID, то пакет отбрасывается.

В режиме Hybrid пользователь может настраивать членство в VLAN, PVID, тегирование, входную фильтрациию и т. д.

По умолчанию Режим Access

Формат switchport mode {access | trunk | hybrid}

Режим Interface Config

no switchport mode

Данная команда возвращает режим работы порта на режим по умолчанию.

Формат no switchport mode

Режим Interface Config

switchport trunk allowed vlan

Используйте эту команду, чтобы настроить список разрешенных VLAN, которые могут принимать и отправлять тегированный трафик на этом интерфейсе в режиме Trunk. По умолчанию - разрешены все.

Список VLAN может быть изменен при помощи функций добавления или удаления, а также заменен другим списком с помощью опций «vlan-list», «all» или «except». Если выбрана опция «all», все VLAN добавляются в список разрешенных. Опция «except» позволяет добавить исключения.

Порты Trunk принимают тегированные пакеты, обрабатывая их согласно содержащемуся в пакете VLAN ID, если данная VLAN находится в списке разрешенных VLAN. Если тегированный пакет получен с идентификатором VLAN, членом которого порт не является, то данный пакет отбрасывается, и запоминания MAC-адреса не происходит. Если VLAN добавляется в систему после настройки порта в режиме Trunk, и и данная VLAN находится в списке разрешенных, эта VLAN автоматически назначается этому порту.

По умолчанию All

Формат switchport trunk allowed vlan {*vlan-list* | all | {add *vlan-list*} | {remove *vlan-list*} | {except *vlan-list* }}

Режим Interface Config

Параметр	Описание
all	Указывает все VLAN от 1 до 4094. Это ключевое слово не разрешено для команд, которые не позволяют одновременно настраивать все VLAN в списке.
add	Добавляет указанный список VLAN к тем спискам, которые уже активны в настоящее время, вместо того, чтобы заменять их.
remove	Удаляет указанный список VLAN из набора уже активных в настоящее время, вместо того, чтобы заменять список. Разрешенный диапазон ID: 1 – 4094, разрешены расширенные VLAN ID форм XY либо X, Y, Z.
except	Перечисляет VLAN, которые должны быть исключены из списка. (Все VLAN, кроме указанных)

Параметр	Описание
vlan-list	Введите VLAN ID либо по одному, либо в виде непрерывного диапазона (определяемого номерами первого и последнего VLAN, через дефис, меньшее значение указывается первым).

no switchport trunk allowed vlan

Данная команда сбрасывает список разрешенных VLAN на порте Trunk на значение списка по умолчанию.

Формат no switchport trunk allowed vlan

Режим Interface Config

switchport trunk native vlan

Используйте эту команду для настройки параметра Native VLAN (PVID) порта Trunk. Функция обрабатывает любые входящие нетегированные пакеты на порте, и тегирует их значением Native VLAN. Native VLAN должна принадлежать к разрешенному списку VLAN для тегирования полученных нетегированных пакетов. В противном случае нетегированные пакеты будут отброшены. Пакеты, отмеченные Native VLAN, передаются через Trunk-порт без тега. Значение по умолчанию - 1.

По умолчанию 1 (VLAN по умолчанию)

Формат switchport trunk native vlan vlan-id

Режим Interface Config

no switchport trunk native vlan

Данная команда возвращает параметр Native VLAN порта Trunk на значение по умолчанию.

Формат no switchport trunk native vlan

Режим Interface Config

switchport access vlan

Данная команда используется для настройки VLAN на порте Access. На порт Access может быть назначена только одна VLAN. По умолчанию порты Access являются членами VLAN 1. При необходимости эти порты могут быть перенастроены на другие VLAN. Удаление Access VLAN на коммутаторе делает порт Access членом VLAN 1. Попытка настроить порт Access на несуществующую VLAN закончится ошибкой, изменения конфигурации не будут сохранены.

По умолчанию 1 (VLAN по умолчанию)

Формат switchport access vlan vlan-id

Режим Interface Config

no switchport access vlan

Данная команда возвращает режим работы порта Access на настройки по умолчанию.

Формат no switchport access vlan

Режим Interface Config

show interface switchport

Данная команда отображает состояние Switchport указанного интерфейса либо всех интерфейсов.

Формат show interfaces switchport unit/slot/port

Режим Privileged EXEC

ПРИМЕР:

(Routing) #show interface switchport 1/0/1

Port: 1/0/1

VLAN Membership Mode: Hybrid

Access Mode VLAN: 1 (default)

Hybrid Mode PVID: 1 (default)

Hybrid Mode Ingress Filtering: Disabled

Hybrid Mode Acceptable Frame Type: Admit all

Hybrid Mode Dynamically Added VLANs:

Hybrid Mode Untagged VLANs: 1

Hybrid Mode Tagged VLANs:

Hybrid Mode Forbidden VLANs:

Trunking Mode Native VLAN: 1 (default)

Trunking Mode Native VLAN tagging: Disable

Trunking Mode VLANs Enabled: All

Protected Port: False

(Routing) #show interfaces switchport

show interface switchport

Данная команда отображает конфигурацию Switchport для выбранного режима и интерфейса. Если интерфейс не указан, будет показана конфигурация для всех интерфейсов.

Формат show interfaces switchport {access | trunk | hybrid} [*unit/slot/port*]

Режим Privileged EXEC

ПРИМЕР:

Switching) # show interface switchport access 1/0/1

```
Intf     PVID
--------- ----
1/0/1    1
```

```
(Switching) # show interface switchport trunk 1/0/6
Intf     PVID    Allowed Vlans List
--------- ----- -------------------
1/0/6    1       All
```

```
(Switching) # show interface switchport hybrid 1/0/5
```

Intf	PVID	Ingress Filtering	Acceptable Frame Type	Untagged Vlans	Tagged Vlans	Forbidden Vlans	Dynamic Vlans
1/0/5	1	Enabled	Admit All	7	10-50,55	9,100-200	88,96

```
(Switching) # show interface switchport hybrid
```

Intf	PVID	Ingress Filtering	Acceptable Frame Type	Untagged Vlans	Tagged Vlans	Forbidden Vlans	Dynamic Vlans
1/0/1	1	Enabled	Admit All	1,4-7	30-40,55	3,100-200	88,96
1/0/2	1	Disabled	Admit All	1	30-40,55	none	none

7.6. Команды Voice VLAN

В этом разделе описаны команды, которые используются для настройки голосовых VLAN (Voice VLAN). Voice VLAN позволяет коммутировать порты для передачи голосового трафика с определенным приоритетом, так же как обеспечить разделение голоса и трафика данных, поступающих на порт. Одним из преимуществ использования Voice VLAN является гарантия стабильного качества передачи звука IP-телефонии при большом потоке данных на порте.

Кроме того, изоляция, предоставляемая самим механизмом работы VLAN, гарантирует, что трафик между VLAN контролируется, и что подключенные к сети клиенты не могут инициировать прямую атаку на компоненты работы голосовой связи. Функция CoS (class of service, основана на QoS IEEE 802.1P) классифицирует и приоритизирует стетевой траффик. Система использует MAC-адрес источника трафика, проходящего через порт, для идентификации потока данных IP-телефона.

voice vlan (Global Config)

Используйте эту команду для включения функции Voice VLAN на коммутаторе.

По умолчанию отключено

Формат voice vlan

Режим Global Config

no voice vlan (Global Config)

Используйте эту команду для отключения функции Voice VLAN на коммутаторе.

Формат no voice vlan

Режим Global Config

voice vlan (Interface Config)

Используйте эту команду для включения функции Voice VLAN для интерфейса либо диапазона интерфейсов.

По умолчанию отключено

Формат voice vlan {vlanid *id* | dot1p *priority* | none | untagged}

Режим Interface Config

Настроить Voice VLAN можно одним из 4 способов:

Параметр	Описание
vlan-id	IP-телефон перенаправляет весь голосовой траффик через определенную VLAN. Диапазон VLAN ID: 1 – 4094 (максимальное количество, поддерживаемое платформой).
dot1p	IP-телефон использует для голосового трафика тегирование 802.1p. Для передачи трафика используется Native VLAN (VLAN 0). Диапазон значений приоритета *priority*: 0 – 7.
none	IP-телефон использует собственную конфигурацию для отправки нетегированного голосового трафика.
untagged	Настроить телефон на передачу нетегированного голосового трафика.

no voice vlan (Interface Config)

Используйте эту команду для отключения функции Voice VLAN на интерфейсе.

Формат no voice vlan

Режим Interface Config

voice vlan data priority

Используйте эту команду, чтобы доверять (trust) или не доверять (untrust) трафику данных, поступающему на интерфейс Voice VLAN или диапазон интерфейсов.

По умолчанию trust (доверять)

Формат voice vlan data priority {untrust | trust}

Режим Interface Config

show voice vlan

Формат show voice vlan [interface {*unit/slot/port* | all}]

Режим Privileged EXEC

Если параметр interface не задан, то отображается лишь глобальный режим Voice VLAN.

Термин	Значение
Administrative Mode	Глобальный режим Voice VLAN.

Когда параметр interface указан:

Термин	Значение
Voice VLAN Mode	Режим работы Voice VLAN на интерфейсе.
Voice VLAN ID	Идентификатор Voice VLAN.
Voice VLAN Priority	Приоритет do1p для Voice VLAN на порте.
Voice VLAN Untagged	Тегирование для трафика Voice VLAN.
Voice VLAN CoS Override	Опция замещения CoS для входящего голосового трафика.
Voice VLAN Status	Рабочее состояние Voice VLAN на порте.

7.7. Команды Provisioning (IEEE 802.1p)

Данный раздел описывает команды, используемые при конфигурировании provisioning (IEEE 802.1p). Данная функция позволяет приоритизировать порты.

vlan port priority all

Эта команда настраивает приоритет порта, назначенный для нетегированных пакетов для всех портов, которые в настоящее время подключены к устройству. Диапазон приоритета: 0 – 7. Любая последующая настройка порта перезаписывает данную конфигурацию.

Формат vlan port priority all *priority*

Режим Global Config

vlan priority

Эта команда настраивает приоритет 802.1p по умолчанию, назначаемый для нетегированных пакетов для определенного интерфейса. Диапазон приоритета: 0 – 7.

По умолчанию 0

Формат vlan priority priority

Режим Interface Config

7.8. Команды защищенных портов

В этом разделе описаны команды, используемые для настройки и просмотра защищенных портов на коммутаторе. Защищенные порты не пересылают трафик друг другу, даже если они находятся в одной и той же VLAN. Однако, защищенные порты могут перенаправлять трафик на все незащищенные порты в своей группе. Незащищенные порты могут перенаправлять трафик на защищенные и незащищенные порты. Порты по умолчанию являются незащищенными.

Если интерфейс сконфигурирован как защищенный порт, и вы добавляете этот интерфейс в Port Channel или Link Aggregation Group (LAG), статус защищенного порта становится функционально отключенным на интерфейсе, а интерфейс принимает конфигурацию порта LAG. Однако конфигурация защищенного порта для интерфейса при этом остается неизменной. Когда интерфейс перестаёт быть членом LAG, конфигурация для этого интерфейса автоматически восстанавливается.

switchport protected (Global Config)

Данная команда создает защищенную группу портов. Параметр **groupid** определяет набор защищенных портов. Пара «**name name**» используется для присвоения имени группе. Имя может быть до 32 символов в длину, и состоять из букв, цифр и пробелов. По умолчанию - пустой текст.

ПРИМЕЧАНИЕ: Защита портов происходит в пределах одного коммутатора. Конфигурация защищенного порта не влияет на трафик между портами на двух разных коммутаторах. Между двумя защищенными портами пересылка трафика не осуществляется.

По умолчанию незащищенный

Формат switchport protected *groupid* name *name*

Режим Global Config

no switchport protected (Global Config)

Данная команда удаляет защищенную группу портов. Параметр **groupid** определяет набор защищенных портов.

Ключевое слово **name** определяет имя для удаления из группы.

Формат no switchport protected *groupid* name

Режим Global Config

switchport protected (Interface Config)

Данная команда добавляет интерфейс к защищенной группе портов. Параметр **groupid** определяет набор защищенных портов, к которым интерфейс будет добавлен. Настроить интерфейс в группе можно только в качестве защищенного.

ПРИМЕЧАНИЕ: Защита портов происходит в пределах одного коммутатора. Конфигурация защищенного порта не влияет на трафик между портами на двух разных

коммутаторах. Между двумя защищенными портами пересылка трафика не осуществляется.

По умолчанию незащищенный

Формат switchport protected *groupid*

Режим Interface Config

no switchport protected (Interface Config)

Данная команда переводит порт в режим незащищенного. Параметр **groupid** определяет набор защищенных портов, из которого интерфейс будет исключен.

Формат no switchport protected *groupid*

Режим Interface Config

show switchport protected

Данная команда отображает состояние всех интерфейсов, включая как защищенные, так и незащищенные.

Формат show switchport protected groupid

Режим Privileged EXEC

User EXEC

Термин	Значение
Group ID	Число, идентифицирующее защищенную группу портов.
Name	Необязательное имя защищенной группы портов Имя может быть до 32 символов в длину, и состоять из букв, цифр и пробелов. По умолчанию - пустой текст.
List of Physical Ports	Список портов, настроенных как защищенные порты для группы, определяемой Group ID. Если для данной группы не настроено ни одного защищенного порта, это поле остаётся пустым.

show interface switchport

Эта команда отображает состояние интерфейса (защищенный/незащищенный) для определенного Group ID.

Формат show interface switchport unit/slot/port groupid

Режим Privileged EXEC

User EXEC

Термин	Значение
Name	Строка, ассоциированная с данной группой для удобства. Она может быть до 32 символов в длину, и состоять из букв, цифр и пробелов. По умолчанию - пустой текст. Данное поле не обязательно для использования.
Protected	Информация о том, защищён ли данный интерфейс или нет. Может быть TRUE или FALSE. Если группа содержит несколько групп, «TRUE» показывается в **groupid** группы.

7.9. Команды GARP

В этом разделе описываются команды, используемые для настройки протокола GARP (Generic Attribute Registration Protocol) и просмотра состояния GARP. Команды в этом разделе влияют как на протокол регистрации GARP VLAN (GVRP), так и на GMRP (GARP Multicast Registration Protocol). GARP - это протокол, который позволяет клиентским станциям регистрироваться с помощью коммутатора для членства в VLAN (с использованием GVMP) или многоадресных группах (с использованием GVMP).

set garp timer join

Эта команда устанавливает время GVRP join для каждого GARP для одного интерфейса, диапазона интерфейсов либо для всех интерфейсов. Время join - это интервал между передачей PDU GARP и регистрацией (или перерегистрацией) членства для группы VLAN или многоадресной группы. Команда действует только при включенном GVRP. Диапазон времени: 10 – 100 сотых секунды. Например, значение 20 означает 0,2 секунды.

По умолчанию 20

Формат set garp timer join *10-100*

Режим Interface Config

Global Config

no set garp timer join

Эта команда сбрасывает интервал отправки GVRP join на значения по умолчанию. Настройки вступают в силу только при включенном GVRP.

Формат no set garp timer join

Режим Interface Config

Global Config

set garp timer leave

Эта команда устанавливает время GVRP leave для интерфейса, диапазона интерфейсов либо для всех интерфейсов. Команда действует только при включенном GVRP. Время GVRP leave - это время ожидания после получения запроса разрегистрации для VLAN или группы многоадресной передачи перед удалением записи VLAN. Это можно рассматривать как буферное время для другого устройства, чтобы заявить о регистрации для того же атрибута. Эта функция помогает в организации бесперебойной работы.

Диапазон времени: 20 – 600 сотых секунды. Например, значение 60 означает 0,6 секунды. Время выхода должно быть минимум втрое больше, нежели время присоединения.

По умолчанию 60

Формат set garp timer leave *20-600*

Режим Interface Config

Global Config

no set garp timer leave

Эта команда сбрасывает время выхода GVRP (leave time) на значения по умолчанию. Настройки вступают в силу только при включенном GVRP.

Формат no set garp timer leave

Режим Interface Config

Global Config

set garp timer leaveall

Данная команда устанавливает частоту генерации сообщений Leave All PDU. Leave All PDU указывает, что все регистрации будут отменены. Для сохранения регистрации все участники должны присоединиться повторно. Значение применяется по портам и по участию GARP. Диапазон времени: 200 – 6000 сотых секунды. Например, значение 1000 означает 10 секунд. Вы можете использовать эту команду на все порты (в режиме Global Config), либо на один порт или диапазон портов (в режиме Interface Config). Настройки вступают в силу только при включенном GVRP. Значение «leave all time» должно быть больше значения «leave time».

По умолчанию 1000

Формат set garp timer leaveall *200-6000*

Режим Interface Config

Global Config

no set garp timer leaveall

Данная команда сбрасывает значение частоты генерации сообщений Leave All PDU на значения по умолчанию. Настройки вступают в силу только при включенном GVRP.

Формат no set garp timer leaveall

Режим Interface Config

Global Config

show garp

Данная команда предоставляет информацию GARP.

Формат show garp

Режимы Privileged EXEC

User EXEC

Термин	Значение
GMRP Admin Mode	Административный режим протокола GMRP (GARP Multicast Registration Protocol) в системе.
GVRP Admin Mode	Административный режим протокола GVRP (GARP VLAN Registration Protocol) в системе.

7.10. Команды GVRP

В этом разделе описаны команды, используемые для настройки и просмотра информации протокола GVRP (GARP VLAN Registration Protocol). Коммутаторы с включенным GVRP обмениваются информацией о конфигурации VLAN, что позволяет GVRP динамически создавать VLAN на trunk-портах и автоматически сокращать структуру VLAN, когда это необходимо.

ПРИМЕЧАНИЕ: При отключенном GVRP система не будет передавать сообщения GVRP.

set gvrp adminmode

Эта команда включает GVRP.

По умолчанию отключено

Формат set gvrp adminmode

Режим Global Config

no set gvrp adminmode

Эта команда отключает GVRP.

Формат no set gvrp adminmode

Режим Global Config

set gvrp interfacemode

Данная команда включает протокол GVRP для одного порта (в режиме Interface Config), диапазона портов (в режиме Interface Range), или всех портов (в режиме Global Config).

По умолчанию отключено

Формат set gvrp interfacemode

Режим Interface Config

Interface Range

Global Config

no set gvrp interfacemode

Данная команда отключает протокол GVRP для одного порта (в режиме Interface Config) либо для всех портов (в режиме Global Config). При отключенном GVRP не будут работать опции Join Time, Leave Time и Leave All Time.

Формат no set gvrp interfacemode

Режим Interface Config

Global Config

show gvrp configuration

Эта команда отображает информацию протокола GARP (Generic Attributes Registration Protocol) для одного или всех интерфейсов.

Формат show gvrp configuration {*unit/slot/port* | all}

Режим Privileged EXEC

User EXEC

Термин	Значение
Interface	unit/slot/port
Join Timer	Интервал между передачей PDU GARP, регистрирующих (или перерегистрирующих) членство для атрибута. Текущие атрибуты - это группа VLAN или многоадресная группа. Существует экземпляр этого таймера для каждого порта и для каждого участника GARP. Допустимые значения: 10 – 100 сотых секунды (от 0,1 до 1,0 секунды). Значение по умолчанию: 20 сотых секунды (0,2 секунды). Минимальный шаг - одна сотая (0,01) секунды.
Leave Timer	Период времени ожидания после получения незарегистрированного запроса атрибута и перед удалением атрибута. Текущие атрибуты - это группа VLAN или многоадресная группа. Это можно рассматривать как буферное время для другого устройства, чтобы заявить о регистрации для того же атрибута. Эта функция помогает в организации бесперебойной работы. Существует экземпляр этого таймера для каждого порта и для каждого участника GARP. Допустимые значения: 20 – 600 сотых секунды (от 0,2 до 6,0 секунды). Значение по умолчанию: 60 сотых секунды (0,6 секунды).
LeaveAll Timer	Данный параметр определяет частоту генерации сообщений LeaveAll PDU. Leave All PDU указывает, что все регистрации будут отменены. Для сохранения регистрации все участники должны присоединиться повторно. Существует экземпляр этого таймера для каждого порта и для каждого участника GARP. Leave All Period Timer настроен на случайное значение в диапазоне от 1 до 1,5 значения LeaveAllTime. Допустимые значения: 200 – 6000 сотых секунды (от 2 до 60 секунды). Значение по умолчанию: 1000 сотых секунды (10 секунд).

Термин	Значение
Port GMRP Mode	Административный режим GMRP для порта. GMRP может быть включен или отключен (по умолчанию). При отключенном параметре не будут работать опции Join Time, Leave Time и Leave All Time.

7.11. Команды GMRP

В этом разделе описаны команды, используемые для настройки и просмотра информации протокола GMRP (GARP Multicast Registration Protocol). Подобно IGMP snooping, GMRP помогает контролировать рассылку многоадресных пакетов. Коммутаторы с включенным GMRP динамически регистрируют и снимают регистрацию информации о членстве в группе с устройствами с MAC-адресацией, прикрепленными к одному и тому же сегменту. GMRP также позволяет распространять информацию о членстве в группах по всем сетевым устройствам в локальной сети с мостовыми соединениями, которая поддерживает службы расширенной фильтрации.

ПРИМЕЧАНИЕ: При отключенном GMRP система не будет пересылать сообщения GMRP.

set gmrp adminmode

Данная команда включает GMRP (GARP Multicast Registration Protocol) в системе.

По умолчанию отключено

Формат set gmrp adminmode

Режим Global Config

no set gmrp adminmode

Данная команда отключает GMRP (GARP Multicast Registration Protocol) в системе.

Формат no set gmrp adminmode

Режим Global Config

set gmrp interfacemode

Эта команда включает GARP Multicast Registration Protocol на одном интерфейсе (режим Interface Config), на диапазоне интерфейсов, либо на всех интерфейсах (режим Global Config). Если интерфейс, поддерживающий GARP, имеет включенную поддержку маршрутизации либо указан как член port-channel (LAG), то функциональность GARP на данном интерфейсе будет отключена. Функциональность GARP повторно включается, если отключается маршрутизация, или порт исключается из членства в port-channel (LAG).

По умолчанию отключено

Формат set gmrp interfacemode

Режим Interface Config

Global Config

no set gmrp interfacemode

Данная команда отключает GARP Multicast Registration Protocol на одном интерфейсе или на всех интерфейсах. Если интерфейс, поддерживающий GARP, имеет включенную поддержку маршрутизации либо указан как член port-channel (LAG), то функциональность GARP на данном интерфейсе будет отключена. Функциональность GARP повторно включается, если отключается маршрутизация, , или порт исключается из членства в port-channel (LAG).

Формат no set gmrp interfacemode

Режим Interface Config

Global Config

show gmrp configuration

Эта команда отображает информацию протокола GMRP (GARP Multicast Registration Protocol) для одного или всех интерфейсов.

Формат show gmrp configuration {*unit/slot/port* | all}

Режим Privileged EXEC

User EXEC

Термин	Значение
Interface	**unit/slot/port** интерфейса, описываемые данной строкой таблицы.
Join Timer	Интервал между передачей блоков PDU GARP, регистрирующих (или перерегистрирующих) членство для атрибута. Текущие атрибуты - это группа VLAN или многоадресная группа. Существует экземпляр этого таймера для каждого порта и для каждого участника GARP. Допустимые значения: 10 – 100 сотых секунды (от 0,1 до 1,0 секунды). Значение по умолчанию: 20 сотых секунды (0,2 секунды). Минимальный шаг - одна сотая (0,01) секунды.
Leave Timer	Период времени ожидания после получения запроса разрегистрации атрибута, перед удалением атрибута. Текущие атрибуты - это группа VLAN или многоадресная группа. Это можно рассматривать как буферное время для другого устройства, чтобы заявить о регистрации для того же атрибута. Эта функция помогает в организации бесперебойной работы. Существует экземпляр этого таймера для каждого порта и для каждого участника GARP. Допустимые значения: 20 – 600 сотых секунды (от 0,2 до 6,0 секунды). Значение по умолчанию: 60 сотых секунды (0,6 секунды).

Термин	Значение
LeaveAll Timer	Данный параметр определяет частоту генерации сообщений LeaveAll PDU. Leave All PDU указывает, что все регистрации будут отменены. Для сохранения регистрации все участники должны присоединиться повторно. Существует экземпляр этого таймера для каждого порта и для каждого участника GARP. Leave All Period Timer настроен на случайное значение в диапазоне от 1 до 1,5 значения LeaveAllTime. Допустимые значения: 200 – 6000 сотых секунды (от 2 до 60 секунды). Значение по умолчанию: 1000 сотых секунды (10 секунд).
Port GMRP Mode	Административный режим GMRP для порта. Может быть включенным или отключенным. При отключенном параметре не будут работать опции Join Time, Leave Time и Leave All Time.

show mac-address-table gmrp

Данная команда отображает записи GMRP в таблице MFDB (Multicast Forwarding Database).

Формат show mac-address-table gmrp

Режим Privileged EXEC

Термин	Значение
VLAN ID	VLAN, в которой узнается MAC-адрес.
MAC Address	Индивидуальный MAC-адрес, для которого коммутатор имеет информацию о передачи или фильтрации. Формат - 6 двухзначных шестнадцатеричных чисел, разделенных двоеточиями, например 01:23:45:67:89:AB.
Type	Тип записи. Статические записи сгенерированы конечным пользователем. Динамические – добавлены в таблицу в результате процесса обучения протокола.
Description	Текстовое описание записи.
Interfaces	Список интерфейсов, предназначенных для передачи (Fwd:) и фильтрации (Flt:).

7.12. Команды управления сетевым доступом на основе порта

В этом разделе описаны команды, который используется для настройки сетевого доступа на основе порта (IEEE 802.1X). Контроль доступа на основе порта позволяет разрешать доступ к сетевым службам только для тех устройство, которые прошли авторизацию и аутентификацию.

aaa authentication dot1x default

Данная команда позволяет настроить метод аутентификации для доступа к коммутатору на основе порта. Дополнительные методы аутентификации используются только в том случае, если предыдущий метод возвращает ошибку (не в том случае, если аутентификация не проходит). Возможные методы:

- ias. Используется база данных внутреннего сервера аутентификации (internal authentication server). Метод может использоваться в сочетании с любым другим методом: **local**, **radius**, и т. д.
- local. Используется локальная база данных пользователей.
- none. Без аутентификации.
- radius. Для аутентификации используется список серверов RADIUS.

Формат aaa authentication dot1x default {[ias]|[*method1 [method2 [method3]]]}*

Режим Global Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) #configure
(Routing) (Config)#aaa authentication dot1x default ias none
(Routing) (Config)#aaa authentication dot1x default ias local radius none
```

clear dot1x statistics

Данная команда сбрасывает статистику 802.1X для указанного порта или для всех портов.

Формат clear dot1x statistics {*unit/slot/port* | all}

Режим Privileged EXEC

clear dot1x authentication-history

Эта команда очищает таблицу истории аутентификации на всех интерфейсах или на указанном интерфейсе.

Формат clear dot1x authentication-history [*unit/slot/port*]

Режим Privileged EXEC

clear radius statistics

Данная команда очищает всю статистику RADIUS.

Формат clear radius statistics

Режим Privileged EXEC

dot1x eapolflood

Используйте эту команду для включения на коммутаторе поддержки EAPOL flood.

По умолчанию отключено

Формат dot1x eapolflood

Режим Global Config

no dot1x eapolflood

Используйте эту команду для отключения поддержки EAPOL flood на коммутаторе.

Формат no dot1x eapolflood

Режим Global Config

dot1x guest-vlan

Данная команда настраивает VLAN как гостевую VLAN (guest vlan) на интерфейсе или диапазоне интерфейсов. Команда определяет активную VLAN как IEEE 802.1X guest VLAN. Диапазон: от 1 до максимального значения VLAN ID, поддерживаемого платформой.

По умолчанию отключено

Формат dot1x guest-vlan *vlan-id*

Режим Interface Config

no dot1x guest-vlan

Эта команда отключает гостевую VLAN на интерфейсе.

По умолчанию отключено

Формат no dot1x guest-vlan

Режим Interface Config

dot1x initialize

Данная команда начинает последовательность инициализации на указанном порте. Команда доступна только в том случае, если метод управления портом - «auto» или «mac-based» (см. ниже). При попытке выполнения в других режимах управления команда возвращает ошибку.

Формат dot1x initialize *unit/slot/port*

Режим Privileged EXEC

dot1x max-req

Эта команда устанавливает максимальное количество попыток передачи аутентификатором фрейма EAPOL EAP Request/Identity перед тем, как отклонить запрос по таймауту. Значение *count* - целое число в диапазоне 1 - 10.

По умолчанию 2

Формат dot1x max-req *count*

Режим Interface Config

no dot1x max-req

Эта команда сбрасывает настроенное максимальное количество попыток передачи аутентификатором фрейма EAPOL EAP Request/Identity на значения по умолчанию.

Формат no dot1x max-req

Режим Interface Config

dot1x port-control

Данная команда устанавливает режим аутентификации для использования на указанном интерфейсе или диапазоне интерфейсов. Параметр **force-unauthorized** - аутентификатор PAE безусловно настраивает порт как неавторизированный. Используйте параметр **force-authorized** для безусловной настройки порта как авторизированного. Параметр **auto** - аутентификатор PAE устанавливает режим управляемого порта, чтобы отражать результаты обмена аутентификацией между стороной, инициировавшей запрос, аутентификатором, и сервером аутентификации. Если указан режим mac-based, на порту устанавливается аутентификация на основе MAC адреса.

По умолчанию auto

Формат dot1x port-control {force-unauthorized | force-authorized | auto | mac-based }

Режим Interface Config

no dot1x port-control

Данная команда сбрасывает режим управления портом 802.1X на настройки по умолчанию.

Формат no dot1x port-control

Режим Interface Config

dot1x port-control all

Данная команда настраивает режим аутентификации для использования на всех портах. Параметр **force-unauthorized** - аутентификатор PAE безусловно настраивает порт как неавторизированный. Используйте параметр **force-authorized** для безусловной настройки порта как авторизированного. Параметр **auto** - аутентификатор PAE устанавливает режим управляемого порта, чтобы отражать результаты обмена аутентификацией между стороной, инициировавшей запрос, аутентификатором, и сервером аутентификации. Если указан режим mac-based, на порту устанавливается аутентификация на основе MAC адреса.

По умолчанию auto

Формат dot1x port-control all {force-unauthorized | force-authorized | auto | mac-based }

Режим Global Config

no dot1x port-control all

Данная команда сбрасывает режим аутентификации на всех портах на настройки по умолчанию.

Формат no dot1x port-control all

Режим Global Config

dot1x mac-auth-bypass

Если на порту установлен режим mac-based, вы можете включить аутентификацию по MAC-адресу (MAB) на интерфейсе. MAB предствляет собой дополнительный механизм аутентификации, который позволяет устройствам, не поддерживающим стандарт 802.1x авторизоваться в сети, используя собственный MAC-адрес в качестве идентификатора. Примером таких устройств являются принтеры, факсы и некоторые IP-телефоны.

По умолчанию отключено

Формат dot1x mac-auth-bypass

Режим Inteface Config

no dot1x mac-auth-bypass

Данная команда сбрасывает аутентификацию по MAC-адресу к настройкам по умолчанию.

Формат dot1x mac-auth-bypass

Режим Inteface Config

dot1x re-authenticate

Данная команда начинает последовательность повторной аутентификации всех устройств за указанным портом либо устройства с выбранным MAC адресом. Команда доступна только в том случае, если метод управления портом - «auto» или «mac-based». При попытке выполнения в других режимах управления команда возвращает ошибку.

Формат dot1x re-authenticate {unit/slot/port | mac-address}

Режим Privileged EXEC

dot1x re-authentication

Данная команда разрешает повторную аутентификацию запрашивающего устройства на указанном интерфейсе или диапазоне интерфейсов.

По умолчанию отключено

Формат dot1x re-authentication

Режим Interface Config

no dot1x re-authentication

Данная команда разрешает повторную аутентификацию на указанном порте.

Формат no dot1x re-authentication

Режим Interface Config

dot1x system-auth-control

Используйте эту команду для включения на коммутаторе поддержки аутентификации dot1x. При отключении конфигурация dot1x не удаляется и остаётся доступной для редактирования.

По умолчанию отключено

Формат dot1x system-auth-control

Режим Global Config

no dot1x system-auth-control

Используйте эту команду для отключения поддержки аутентификации dot1x на коммутаторе.

Формат no dot1x system-auth-control

Режим Global Config

dot1x system-auth-control monitor

Используйте эту команду для включения на коммутаторе режима мониторинга 802.1X. Назначение режима мониторинга - помочь устранить проблемы с настройкой аутентификации на основе порта, не нарушая доступа к сети для хостов, подключенных к коммутатору. В режиме мониторинга хосту предоставляется сетевой доступ к порту с поддержкой 802.1X, даже если он не прошел процесс аутентификации. Результаты процесса регистрируются для диагностических целей.

По умолчанию отключено

Формат dot1x system-auth-control monitor

Режим Global Config

no dot1x system-auth-control monitor

Используйте эту команду для отключения режима мониторинга 802.1X на коммутаторе.

Формат no dot1x system-auth-control monitor

Режим Global Config

dot1x timeout

Эта команда устанавливает значение таймера (в секундах), используемого конечным автоматом аутентификатора, на интерфейсе или диапазоне интерфейсов. В зависимости от используемого токена и значения (в секундах) задаются различные параметры времени ожидания. Поддерживаются следующие токены:

Токены	Значение
guest-vlanperiod	Время (в секундах), в течение которого аутентификатор ожидает получения каких-либо пакетов EAPOL на порте, до авторизации порта и размещения его в гостевой vlan (если настроена). Таймер гостевой vlan применим только тогда, когда гостевая vlan настроена на этом конкретном порту.

Токены	Значение
reauth-period	Значение таймера (в секундах), используемое конечным автоматом аутентификатора на этом порту, чтобы определить, когда происходит повторная аутентификация запрашивающего устройства. Значение должно принадлежать диапазону 1 – 65535.
quiet-period	Значение таймера (в секундах), используемое конечным автоматом аутентификатора на этом порту, чтобы определить периоды времени, в течение которых не будет производиться попыток подключения запрашивающего устройства. Значение должно принадлежать диапазону 0 – 65535.
tx-period	Значение таймера (в секундах), используемое конечным автоматом аутентификатора на этом порту, чтобы определить, когда отправить запрос EAPOL EAP Request/Identity к запрашивающему устройству. Значение должно принадлежать диапазону 1 – 65535.
supp-timeout	Значение таймера (в секундах), используемое конечным автоматом аутентификатора на этом порту, чтобы определить время отключения запрашивающего устройства по таймауту. Значение должно принадлежать диапазону 1 – 65535.
server-timeout	Значение таймера (в секундах), используемое конечным автоматом аутентификатора на этом порту для определения таймаута сервера аутентификации. Значение должно принадлежать диапазону 1 – 65535.
По умолчанию	guest-vlan-period: 90 секунд reauth-period: 3600 секунд quiet-period: 60 секунд tx-period: 30 секунд supp-timeout: 30 секунд server-timeout: 30 секунд
Формат	dot1x timeout {{guest-vlan-period *seconds*} |{reauth-period *seconds*} | {quiet-period *seconds*} | {tx-period *seconds*} | {supp-timeout *seconds*} | {server-timeout *seconds*}}
Режим	Interface Config

no dot1x timeout

Эта команда сбрасывает значения таймера (в секундах), используемые конечным автоматом аутентификатора, на значения по умолчанию. В зависимости от токена, будут установлены соответствующие значения по умолчанию.

Формат no dot1x timeout {guest-vlan-period | reauth-period | quiet-period | tx-period | supptimeout | server-timeout}

Режим Interface Config

dot1x unauthenticated-vlan

Используйте эту команду для настройки неаутентифицированной VLAN, связанной с указанным интерфейсом или диапазоном интерфейсов. ID неаутентифицированной VLAN может быть действительным VLAN ID, в диапазоне от нуля до максимального поддерживаемого значения VLAN ID (4094). Неаутентифицированная VLAN должна быть настроена в базе данных VLAN статически. По умолчанию неаутентифицированная VLAN имеет ID 0 (то есть не работает).

По умолчанию 0

Формат dot1x unauthenticated-vlan *vlan id*

Режим Interface Config

no dot1x unauthenticated-vlan

Данная команда сбрасывает настройки неаутентифицированной VLAN, связанной с интерфейсом, на значения по умолчанию.

Формат no dot1x unauthenticated-vlan

Режим Interface Config

dot1x critical-vlan

Используйте эту команду для настройки аварийной VLAN, связанной с указанным интерфейсом или диапазоном интерфейсов. ID аварийной VLAN может быть действительным VLAN ID, в диапазоне от нуля до максимального поддерживаемого значения VLAN ID (4094). Аварийная VLAN должна быть настроена в базе данных VLAN статически. По умолчанию аварийная VLAN имеет ID 0 (то есть не работает).

По умолчанию 0

Формат dot1x unauthenticated-vlan vlan id

Режим Interface Config

no dot1x critical-vlan

Данная команда сбрасывает настройки аварийной VLAN, связанной с интерфейсом, на значения по умолчанию.

Формат no dot1x critical-vlan

Режим Interface Config

dot1x user

Данная команда добавляет указанного пользователя в список пользователей, имеющих доступ к указанному порту или всем портам. **user** - настроенный пользователь.

Формат dot1x user *user* {*unit/slot/port* | all}

Режим Global Config

no dot1x user

Данная команда удаляет указанного пользователя из списка пользователей, имеющих доступ к указанному порту или всем портам.

Формат no dot1x user *user* {*unit/slot/port* | all}

Режим Global Config

show authentication methods

Данная команда отображает информацию о методах аутентификации.

Формат show authentication methods

Режим Privileged EXEC

Термин	Значение
Authentication Login List	Имя списка логинов аутентификации.
Method 1	Первый метод в списке, если имеется.
Method 2	Второй метод в списке, если имеется.
Method 3	Третий метод в списке, если имеется.

ПРИМЕР: Следующий пример показывает настройки аутентификации.

```
(switch)#show authentication methods
Login Authentication Method Lists
---------------------------------
defaultList              : local
networkList              : local

Enable Authentication Method       Lists
---------------------------------
enableList               : enable       none
enableNetList            : enable       deny
Line        Login Method List            Enable Method List
------- -----------------  ------------------
Console     defaultList                   enableList
Telnet      networkList                   enableNetList
SSH         networkList                   enableNetList
HTTPS             :local
HTTP              :local
DOT1X             :
```

show dot1x

Данная команда используется для отображения сводной информации о глобальной конфигурации dot1x, сводной информации о конфигурации dot1x для определенного порта или всех портов, подробной конфигурации dot1x для указанного порта и статистики dot1x для указанного порта - в зависимости от используемых токенов.

Формат show dot1x [{summary {unit/slot/port | all} | detail unit/slot/port | statistics unit/slot/port]

Режим Privileged EXEC

Если не использовать необязательные параметры *unit/slot/port* либо *vlanid*, команда отобразит глобальный режим dot1x, режим назначения VLANи режим создания динамических VLAN.

Термин	Значение
Administrative Mode	Указывает, включена или выключена функция аутентификации на коммутаторе.
VLAN Assignment Mode	Указывает, разрешено ли назначение авторизованного порта в сеть VLAN, назначенную RADIUS.
Dynamic VLAN Creation Mode	Указывает, может ли коммутатор динамически создавать VLAN, назначенные RADIUS, если их не существует на коммутаторое.
Monitor Mode	Указывает, включен или выключен на коммутаторе режим мониторинга Dot1x.

При использовании необязательного параметра **summary {unit/slot/port | all}** конфигурация dot1x будет показана для конкретного порта либо для всех портов.

Термин	Значение
Interface	Интерфейс, конфигурация которого отображается.
Control Mode	Настроенный режим управления для данного порта. Возможные значения: force-unauthorized | force-authorized | auto | mac-based.
Operating Control Mode	Режим управления, активный для данного порта. Возможные значения: authorized | unauthorized.
Reauthentication Enabled	Указывает, включена ли для данного порта повторная аутентификация.
Port Status	Указывает авторизован или не авторизован порт. Возможные значения: authorized | unauthorized.

ПРИМЕР: Выполнение команды show dot1x.

summary 0/1.

Interface	Control Mode	Operating Control Mode	Port Status
---	---	---	---
0/1	auto	auto	Authorized

При использовании необязательного параметра 'detail *unit/slot/port*' конфигурация dot1x будет показана для конкретного порта.

Термин	Значение
Port	Интерфейс, конфигурация которого отображается.
Protocol Version	Версия протокола, ассоциируемая с этим портом. Единственное возможное значение - 1, соответствующее первой версии спецификации dot1x.
PAE Capabilities	Функциональность PAE (port access entity) для этого порта. Возможные значения: Authenticator либо Supplicant.
Control Mode	Настроенный режим управления для данного порта. Возможные значения: force-unauthorized | force-authorized | auto | mac-based.
Authenticator PAE State	Текущее состояние конечного автомата аутентификатора PAE. Возможные значения: Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized и ForceUnauthorized.
Backend Authentication State	Текущее состояние фонового конечного автомата аутентификатора. Возможные значения: Request, Response, Success, Fail, Timeout, Idle и Initialize.
Quiet Period	Таймер, используемый конечным автоматом аутентификатора на этом порту, чтобы определить периоды времени, в течение которых не будет производиться попыток подключения запрашивающего устройства. Возможный диапазон значений: 0 – 65535 (в секундах).
Transmit Period	Таймер, используемый конечным автоматом аутентификатора на этом порту, чтобы определить, когда отправить запрос EAPOL EAP Request/Identity к запрашивающему устройству. Возможный диапазон значений: 1 – 65535 (в секундах).
Guest-VLAN ID	Настроенный на интерфейсе идентификатор гостевой VLAN.

Термин	Значение
Guest VLAN Period	Время в секундах, которое аутентификатор ждет до авторизации и размещения порта в гостевой VLAN, если на этом порте не обнаружены пакеты EAPOL.
Supplicant Timeout	Таймер таймаута, используемый конечным автоматом аутентификатора на данном порте для запрашивающего устройства Возможный диапазон значений: 1 – 65535 (в секундах).
Server Timeout	Таймер таймаута, используемый конечным автоматом аутентификатора на данном порте для сервера аутентификации по таймауту. Возможный диапазон значений: 1 – 65535 (в секундах).
Maximum Requests	Максимальное количество попыток передачи аутентификатором фрейма EAPOL EAP Request/Identity перед тем, как отклонить запрашивающее устройство по таймауту. Возможный диапазон значений: 1 – 10.
Configured MAB Mode	Административный режим функции MAC authentication bypass на коммутаторе.
Operational MAB Mode	Рабочий режим функции MAC authentication bypass на коммутаторе. MAB может быть включенным, но при этом не работать - если режим управления не основан на MAC.
Vlan-ID	VLAN, назначенный на порт сервером RADIUS.
VLAN Assigned Reason	Причина, по которой VLAN, указанная в поле VLAN-ID, была назначена на порт. Возможные значения: RADIUS, Unauthenticated VLAN, Guest VLAN, default и Not Assigned. Когда VLAN Assigned Reason имеет причину «Not Assigned», это означает, что порт не был назначен ни одной из VLAN через dot1x.
Reauthentication Period	Таймер используемый конечным автоматом аутентификатора на данном порте для того чтобы определить, когда будет совершена повторная аутентификация. Возможный диапазон значений: 1 – 65535 (в секундах).
Reauthentication Enabled	Указывает, включена ли для данного порта повторная аутентификация. Возможные значения: ‘True” или “False”.
Key Transmission Enabled	Указывает, передаётся ли ключ запрашивающему устройству на указанный порт. Возможные значения: True или False.

Термин	Значение
EAPOL Flood Mode Enabled	Указывает, включена ли на коммутаторе поддержка EAPOL flood. Возможные значения: True или False.
Control Direction	Направление управления для указанного порта или диапазона портов. Возможные значения: both или in.
Maximum Users	Максимальное колиество клиентов, которые могут пройти аутентификацию на порте с режимом dot1x, основанном на MAC.
Unauthenticated VLAN ID	Указывает, настроена ли на данном порте неаутентифицированная VLAN.
Critical VLAN ID	Указывает, настроена ли на данном порте аварийная VLAN.
Session Timeout	Указывает время, в течение которого данная сессия действительна. Период времени (в секундах) возвращается сервером RADIUS при аутентификации на порте.
Session Termination Action	Это значение указывает на действие, которое необходимо предпринять по истечении времени ожидания сеанса. Возможные значения: Default, Radius-Request. «Default» - сессия прерывается, порт переходит в неавторизированное состояние. «Radius-Request» - производится повторная аутентификация клиента на порте.

ПРИМЕР: Вывод командной строки для данной команды.

```
(switch) #show dot1x detail 1/0/3
Port..... 1/0/1
Protocol Version..... 1
PAE Capabilities..... Authenticator
Control Mode..... auto
Authenticator PAE State..... Initialize
Backend Authentication State..... Initialize
Quiet Period (secs)..... 60
Transmit Period (secs)..... 30
Guest VLAN ID..... 0
Guest VLAN Period (secs)..... 90
Supplicant Timeout (secs)..... 30
Server Timeout (secs)..... 30
Maximum Requests..... 2
Configured MAB Mode..... Enabled
```

Operational MAB Mode..... Disabled
VLAN Id..... 0
VLAN Assigned Reason ..... Not Assigned
Reauthentication Period (secs) 3600
Reauthentication Enabled..... FALSE
Key Transmission Enabled ..... FALSE
EAPOL flood Mode Enabled..... FALSE
Control Direction ..... both
Maximum Users..... 16
Unauthenticated VLAN ID..... 0
Session Timeout..... 0
Critical VLAN ID 0
Session Termination Action ..... Default

При использовании необязательного параметра **'statistics unit/slot/port'** конфигурация dot1x будет показана для конкретного порта.

Термин	Значение
Port	Интерфейс, для которого отображается статистика.
EAPOL Frames Received	Количество верных фреймов EAPOL любого типа, полученных этим аутентификатором.
EAPOL Frames Transmitted	Количество фреймов EAPOL любого типа, переданных этим аутентификатором.
EAPOL Start Frames Received	Количество начальных фреймов EAPOL, полученных этим аутентификатором.
EAPOL Logoff Frames Received	Количество logoff-фреймов EAPOL, полученных этим аутентификатором.
Термин	Значение
Last EAPOL Frame Version	Номер версии протокола в последнем полученном фрейме EAPOL.
Last EAPOL Frame Source	MAC-источника в последнем полученном фрейме EAPOL.
EAP Response/ Id Frames Received	Количество фреймов EAPOL response/identity, полученных этим аутентификатором.

Термин	Значение
EAP Response Frames Received	Количество верных ответных фреймов EAPOL (кроме фреймов response/id), полученных этим аутентификатором.
EAP Request/Id Frames Transmitted	Количество фреймов EAPOL response/identity, отправленных этим аутентификатором.
EAP Request Frames Transmitted	Количество фреймов запроса EAPOL (кроме фреймов response/identity), отправленных этим аутентификатором.
Invalid EAPOL Frames Received	Количество фреймов EAPOL неопознанного типа, полученных этим аутентификатором.
EAP Length Error Frames Received	Количество фреймов EAPOL неопознанного типа, полученных этим аутентификатором.

show dot1x authentication-history

Данная команда отображает события и информацию аутентификации 802.1X для всех интерфейсов или указанного интерфейса. Использование необязательных ключевых слов позволяет отображать только события ошибок аутентификации в краткой или подробной формах.

Формат show dot1x authentication-history {unit/slot/port | all} [failed-auth-only] [detail]

Режим Privileged EXEC

Термин	Значение
Time Stamp	Точное время события.
Interface	Физический порт, на котором происходит событие.
Mac-Address	MAC-адрес клиента/запрашивающего устройства.
VLAN assigned	Сеть VLAN, назначенная клиенту/порту при аутентификации.
VLAN assigned Reason	Тип назначенного VLAN ID, который может иметь следующие значения: Guest VLAN, Unauth, Default, RADIUS Assigned либо Montior Mode VLAN ID.
Auth Status	Состояние аутентификации.
Reason	Фактическая причина успешной либо безуспешной аутентификации.

show dot1x clients

Данная команда предоставляет информацию о клиентах 802.1X. Также команда отображает информацию о количестве клиентов, аутентифицированных в режиме мониторинга (Monitor mode) и использующих 802.1X.

Формат show dot1x clients {*unit/slot/port* | all}

Режим Privileged EXEC

Термин	Значение
Clients Authenticated using Monitor Mode	Количество клиентов Dot1x, аутентифицированных в режиме мониторинга.
Clients Authenticated using Dot1x	Количество клиентов Dot1x, аутентифицированных при помощи процесса 802.1x
Logical Interface	Логический номер порта, ассоциированный с клиентом.
Interface	Физический порт, с которым ассоциировано запрашивающее устройство.
User Name	Имя пользователя, используемое клиентом для аутентификации на сервере.
Supplicant MAC Address	MAC-адрес запрашивающего устройства.
Session Time	Время, прошедшее с момента последнего входа запрашивающего устройства.
Filter ID	Указывает Filter ID, возвращенный сервером RADIUS при аутентификации клиента. Является настроенным именем политики DiffServ на коммутаторе.
VLAN ID	Сеть VLAN, назначенная порту.
VLAN Assigned	Причина, по которой VLAN, идентифицированная в поле VLAN ID, была назначена порту. Возможные значения: RADIUS, Unauthenticated VLAN, Monitor Mode или Default. Когда причиной назначения VLAN является «Default», это означает, что VLAN была назначена порту, поскольку P-VID этого порта был этот VLAN ID.
Session Timeout	Указывает время, в течение которого данная сессия действительна. Период времени (в секундах) возвращается сервером RADIUS при аутентификации на порте.

Термин	Значение
Session Termination action	Это значение указывает на действие, которое необходимо предпринять по истечении таймаута сессии. Возможные значения: Default, Radius-Request. «Default» - сессия прерывается, информация о клиенте очищается. «Radius-Request» - производится повторная аутентификация клиента.

show dot1x users

Данная команда отображает пользовательскую информацию 802.1X о безопасности порта для локально настроенных пользователей.

Формат show dot1x users *unit/slot/port*

Режим Privileged EXEC

Термин	Значение
Users	Локально настроенные пользователи для доступа к указанному порту.

7.13. Команды запрашивающего устройства 802.1X

Коммутатор поддерживает функциональность запрашивающего устройства 802.1X (dot1x) на портах «точка-точка». Администратор может настроить имя пользователя и пароль для аутентификации, а также возможности запрашивающего порта.

dot1x pae

Данная команда устанавливает роль порта в dot1x. Порт может иметь статус supplicant (запрашивающий) либо authenticator (аутентификатор).

Формат dot1x pae {supplicant | authenticator}

Режим Interface Config

dot1x supplicant port-control

Данная команда устанавливает статус авторизации порта (авторизованный или неавторизованный). Сделть это можно как вручную, так и путем настройки порта на автоматическую авторизацию после загрузки. Все порты являются аутентификаторами по умолчанию. Если необходимо перенести атрибуты порта с <authenticator to supplicant> либо <supplicant to authenticator>, используйте эту команду.

Формат dot1x supplicant port-control {auto | force-authorized | force_unauthorized}

Режим Interface Config

Параметр	Описание
auto	Порт находится в состоянии Unauthorized (неавторизированный), пока он не представит свои учетные данные имени пользователя и пароля аутентификатору. Если аутентификатор авторизирует порт, он переходит в состояние Authorized (авторизированный).
force-authorized	Устанавливает состояние авторизации порта на Авторизованный, минуя процесс аутентификации.
force-unauthorized	Устанавливает состояние авторизации порта на Неавторизованный, минуя процесс аутентификации.

no dot1x supplicant port-control

Данная команда сбрасывает режим управления портом на настройки по умолчанию.

По умолчанию auto

Формат no dot1x supplicant port-control

Режим Interface Config

dot1x supplicant max-start

Эта команда настраивает количество попыток запрашивающего устройства найти аутентификатор, перед тем как сделать вывод об отсутствии аутентификатора.

По умолчанию 3

Формат dot1x supplicant max-start *<1-10>*

Режим Interface Config

no dot1x supplicant max-start

Данная команда сбрасывает значения max-start на значения по умолчанию.

Формат no dot1x supplicant max-start

Режим Interface Config

dot1x supplicant timeout start-period

Данная команда настраивает интервал таймера начала периода ожидания запроса идентификации EAP от аутентификатора.

По умолчанию 30 секунд

Формат dot1x supplicant timeout start-period <1-65535 seconds>

Режим Interface Config

no dot1x supplicant timeout start-period

Данная команда сбрасывает значение таймера начала периода на настройки по умолчанию.

Формат no dot1x supplicant timeout start-period

Режим Interface Config

dot1x supplicant timeout held-period

Данная команда настраивает интервал таймера периода удержания для ожидания следующей аутентификации после неудачной предыдущей попытки.

По умолчанию 60 секунд

Формат dot1x supplicant timeout held-period <1-65535 seconds>

Режим Interface Config

no dot1x supplicant timeout held-period

Данная команда сбрасывает значение таймера периода удержания на настройки по умолчанию.

Формат no dot1x supplicant timeout held-period

Режим Interface Config

dot1x supplicant timeout auth-period

Данная команда настраивает интервал таймера периода аутентификации для ожидания следующего запроса идентификации EAP от аутентификатора.

По умолчанию 30 секунд

Формат dot1x supplicant timeout auth-period <1-65535 seconds>

Режим Interface Config

no dot1x supplicant timeout auth-period

Данная команда сбрасывает значение таймера периода аутентификации на настройки по умолчанию.

Формат no dot1x supplicant timeout auth-period

Режим Interface Config

dot1x supplicant user

Данная команда используется для сопоставления заданного пользователя с портом.

Формат dot1x supplicant user

Режим Interface Config

show dot1x statistics

Данная команда отображает детальную статистику dot1x.

Формат show dot1x statistics unit/slot/port

Режимы Privileged EXEC

User EXEC

Термин	Значение
EAPOL Frames Received	Количество верных фреймов EAPOL, полученных на порте.
EAPOL Frames Transmitted	Количество фреймов EAPOL, переданных через порт.
EAPOL Start Frames Transmitted	Количество начальных фреймов EAPOL, переданных через порт.
EAPOL Logoff Frames Received	Количество фреймов Log off EAPOL, полученных на порте.
EAP Resp/ID Frames Received	Количество фреймов EAP Respond ID, полученных на порте.
EAP Response Frames Received	Количество верных фреймов EAP Respond, полученных на порте.
EAP Req/ID Frames Transmitted	Количество фреймов EAP Requested ID, переданных через порт.
EAP Req Frames Transmitted	Количество фреймов EAP Request, переданных через порт.
Термин	Значение
Invalid EAPOL Frames Received	Количество нераспознанных фреймов EAPOL, полученных на порте.
EAP Length Error Frames Received	Количество фреймов EAPOL с некорректной длиной пакета, полученных на порте.
Last EAPOL Frames Version	Номер версии протокола последнем недавно полученном фрейме EAPOL.

Термин	Значение
Last EAPOL Frames Source	MAC-источника в последнем недавно полученном фрейме EAPOL.

ПРИМЕР: Вывод командной строки для данной команды.

```
(switch) #show dot1x statistics 0/1
Port..... 0/1
EAPOL Frames Received ..... 0
EAPOL Frames Transmitted..... 0
EAPOL Start Frames Transmitted ..... 3
EAPOL Logoff Frames Received ..... 0
EAP Resp/Id frames transmitted..... 0
EAP Response frames transmitted ..... 0
EAP Req/Id frames transmitted ..... 0
EAP Req frames transmitted..... 0
Invalid EAPOL frames received..... 0
EAP length error frames received ..... 0
Last EAPOL Frame Version..... 0
Last EAPOL Frame Source..... 00:00:00:00:02:01
```

7.14. Команды Storm-Control

В этом разделе описываются команды, используемые для настройки и просмотра конфигурации функции Storm-Control. Штормом трафика называется ситуация, когда входящие пакеты наводняют локальную сеть, что приводит к ухудшению производительности. Для предотвращения этой ситуации существует функция Storm-Control.

Коммутатор обеспечивает предотвращение шторма для широковещательной, многоадресной и одноадресной передачи для отдельных интерфейсов. Unicast StormControl защищает от трафика с неизвестными системе MAC-адресами. Функции Broadcast, Multicast и Unicast Storm-Control отбрасывают трафик в том случае, если скорость входящего трафика на интерфейсе начинает превышать настроенный для данного типа порог.

Для активирования функции Storm-Control включите ее для всех или для определенных интерфейсов, и установите пороговые значения отключения широковещательного, многоадресного или одноадресного трафика. Функция Storm-Control позволяет вам ограничить скорость прохождения конкретных типов пакетов через коммутатор по порту и по типу.

При настройке уровня Storm-Control определенного типа происходит автоматическое включение данного типа. Отключение функции (с использованием «no»-версии команды) настраивает уровни Storm-Control на значения по умолчанию. Использование «**no**»-версии команды «**storm-control**» без указания уровня («level») отключает данную форму предтвращения шторма, но сохраняет настроенный уровень. Таким образом, при следующей активации функции будут применены сохраненные настройки.

ПРИМЕЧАНИЕ: Фактическая скорость входящего трафика, необходимого для активации StormControl, основана на размере входящих пакетов и жестко запрограммированного среднего размера пакета в 512 байт - используется для вычисления скорости прохождения пакетов в секунду (pps) - т.к. для плоскости передачи требуется скорость в pps, а не в Кбит/с. Например, если настроенный предел составляет 10%, он преобразуется в ~ 25000 pps, и этот предел в pps устанавливается для передачи (аппаратно). Результат, близкий к желаемому, можно получить при использовании пакетов объемом 512 байт.

storm-control broadcast

Данная команда активирует функцию противодействия широковещательным штормам на всех интерфейсах (в режиме Global Config) либо на одном или нескольких интерфейсах (в режиме Interface Config). При включенной функции подавления широковещательных штормов трафик отбрасывается при превышении указанного порога входящим широковещательным трафиком. Таким образом, значение порога регулирует входящий широковещательный трафик.

По умолчанию	отключено
Формат	storm-control broadcast
Режим	Global Config
	Interface Config

no storm-control broadcast

Данная команда отключает функцию противодействия широковещательным штормам на всех интерфейсах (в режиме Global Config) либо на одном или нескольких интерфейсах (в режиме Interface Config).

Формат	no storm-control broadcast
Режим	Global Config
	Interface Config

storm-control broadcast action

Данная команда настраивает действие, выполняемое в ответ на обнаружение широковещательного шторма: shutdown либо trap . Действие команды распространяется на все интерфейсы (в режиме Global Config) либо на один или несколько интерфейсов (в режиме Interface Config). Опция shutdown - отключить интерфейс при поступлении входящих широковещательных пакетов со скоростью большей, чем предусмотрено значением порога. Опция trap - интерфейс отравляет trap-сообщение приблизительно каждые 30 секунд, до тех пор, пока широковещательный шторм не прекратится.

По умолчанию	Нет
Формат	storm-control broadcast action {shutdown | trap}
Режим	Global Config
	Interface Config

no storm-control broadcast action

Данная команда возвращает настройки действия, выполняемое в ответ на обнаружение широковещательного шторма, на значения по умолчанию.

Формат no storm-control broadcast action

Режим Global Config

Interface Config

storm-control broadcast level

Данная команда настраивает порог обнаружения широковещательного шторма для всех интерфейсов (в режиме Global Config) либо для одного или нескольких интерфейсов (в режиме Interface Config), как процент от скорости линка. При включенной функции подавления широковещательных штормов трафик отбрасывается при превышении указанного порога входящим широковещательным трафиком. Таким образом, значение порога регулирует входящий широковещательный трафик.

По умолчанию 5

Формат storm-control broadcast level *0-100*

Режим Global Config

Interface Config

no storm-control broadcast level

Данная команда возвращает значение порога обнаружения широковещательного шторма на значения по умолчанию для всех интерфейсов (в режиме Global Config) либо для одного или нескольких интерфейсов (в режиме Interface Config). Функция обнаружения широковещательного шторма отключается.

Формат no storm-control broadcast level

Режим Global Config

Interface Config

storm-control broadcast rate

Данная команда позволяет настроить порог обнаружения широковещательного шторма на всех интерфейсах (в режиме Global Config) либо на одном или нескольких интерфейсах (в режиме Interface Config), в пакетах в секунду (pps). При включенной функции подавления широковещательных штормов трафик отбрасывается при превышении указанного порога входящим широковещательным трафиком уровня 2 OSI. Таким образом, значение порога регулирует входящий широковещательный трафик.

По умолчанию 0

Формат storm-control broadcast rate *0*-14880000

Режим Global Config

Interface Config

no storm-control broadcast rate

Данная команда возвращает значение порога обнаружения широковещательного шторма на значения по умолчанию для всех интерфейсов (в режиме Global Config) либо для одного или нескольких интерфейсов (в режиме Interface Config). Функция обнаружения широковещательного шторма отключается.

Формат no storm-control broadcast rate

Режим Global Config

Interface Config

storm-control multicast

Данная команда активирует функцию противодействия многоадресным штормам на всех интерфейсах (в режиме Global Config) либо на одном или нескольких интерфейсах (в режиме Interface Config). При включенной функции подавления многоадресных штормов трафик отбрасывается при превышении указанного порога входящим многоадресным трафиком. Таким образом, значение порога регулирует входящий многоадресный трафик.

По умолчанию отключено

Формат storm-control multicast

Режим Global Config

Interface Config

no storm-control multicast

Данная команда отключает функцию противодействия многоадресным штормам на всех интерфейсах (в режиме Global Config) либо на одном или нескольких интерфейсах (в режиме Interface Config).

Формат no storm-control multicast

Режим Global Config

Interface Config

storm-control multicast action

Данная команда настраивает действие, выполняемое в ответ на обнаружение многоадресного шторма: **shutdown** либо trap . Действие команды распространяется на все интерфейсы (в режиме Global Config) либо на один или несколько интерфейсов (в режиме Interface Config). Опция **shutdown** - отключить интерфейс при поступлении входящих многоадресных пакетов со скоростью большей, чем предусмотрено значением порога. Опция **trap** - интерфейс отравляет trap-сообщение приблизительно каждые 30 секунд до тех пор, пока многоадресный шторм не прекратится.

По умолчанию Нет

Формат storm-control multicast action {shutdown | trap}

Режим Global Config

Interface Config

no storm-control multicast action

Данная команда возвращает настройки действия, выполняемые в ответ на обнаружение многоадресного шторма, на значения по умолчанию.

Формат no storm-control multicast action

Режим Global Config

Interface Config

storm-control multicast level

Данная команда настраивает порог обнаружения многоадресного шторма для всех интерфейсов (в режиме Global Config) либо для одного или нескольких интерфейсов (в режиме Interface Config Режим) в процентах от скорости линка. При включенной функции подавления многоадресных штормов трафик отбрасывается при превышении указанного порога входящим многоадресным трафиком. Таким образом, значение порога регулирует входящий многоадресный трафик.

По умолчанию 5

Формат storm-control multicast level *0-100*

Режим Global Config

Interface Config

no storm-control multicast level

Данная команда возвращает значение порога обнаружения многоадресного шторма на значения по умолчанию для всех интерфейсов (в режиме Global Config) либо для одного или нескольких интерфейсов (в режиме Interface Config). Функция обнаружения многоадресного шторма отключается.

Формат no storm-control multicast level *0-100*

Режим Global Config

Interface Config

storm-control multicast rate

Данная команда позволяет настроить порог обнаружения многоадресного шторма на всех интерфейсах (в режиме Global Config) либо на одном или нескольких интерфейсах (в режиме Interface Config), в пакетах в секунду (pps). При включенной функции подавления многоадресных штормов трафик отбрасывается при превышении указанного порога входящим многоадресным трафиком уровня 2 OSI. Таким образом, значение порога регулирует входящий многоадресный трафик.

По умолчанию 0

Формат storm-control multicast rate *0*-14880000

Режим Global Config

Interface Config

no storm-control multicast rate

Данная команда возвращает значение порога обнаружения многоадресного шторма на значения по умолчанию для всех интерфейсов (в режиме Global Config) либо для одного или нескольких интерфейсов (в режиме Interface Config). Функция обнаружения многоадресного шторма отключается.

Формат no storm-control multicast rate

Режим Global Config

Interface Config

storm-control unicast

Данная команда активирует функцию противодействия одноадресным штормам на всех интерфейсах (в режиме Global Config) либо на одном или нескольких интерфейсах (в режиме Interface Config). При включенной функции подавления одноадресных штормов неизвестный трафик отбрасывается при превышении указанного порога входящим одноадресным трафиком уровня 2 OSI. Таким образом, значение порога регулирует входящий неизвестный одноадресный трафик.

По умолчанию отключено

Формат storm-control unicast

Режим Global Config

Interface Config

no storm-control unicast

Данная команда отключает функцию противодействия одноадресным штормам на всех интерфейсах (в режиме Global Config) либо на одном или нескольких интерфейсах (в режиме Interface Config).

Формат no storm-control unicast

Режим Global Config

Interface Config

storm-control unicast action

Данная команда настраивает действие, выполняемое в ответ на обнаружение одноадресного шторма: shutdown либо trap . Действие команды распространяется на все интерфейсы (в режиме Global Config) либо на один или несколько интерфейсов (в режиме Interface Config). Опция shutdown - отключить интерфейс при поступлении входящих одноадресных пакетов со скоростью большей, чем предусмотрено значением порога. Опция trap - интерфейс отравляет trap-сообщение приблизительно каждые 30 секунд до тех пор, пока одноадресный шторм не прекратится.

По умолчанию Нет

Формат storm-control unicast action {shutdown | trap}

Режим Global Config

Interface Config

no storm-control unicast action

Данная команда возвращает настройки действия, выполняемое в ответ на обнаружение одноадресного шторма, на значения по умолчанию.

Формат no storm-control unicast action

Режим Global Config

Interface Config

storm-control unicast level

Данная команда настраивает порог обнаружения одноадресного шторма для всех интерфейсов (в режиме Global Config) либо для одного или нескольких интерфейсов (в режиме Interface) в процентах от скорости линка. При включенной функции подавления одноадресных штормов неизвестный трафик отбрасывается при превышении указанного порога входящим неизвестным одноадресным трафиком уровня 2 OSI. Таким образом, значение порога регулирует входящий неизвестный одноадресный трафик. Команда также активирует режим обнаружения одноадресного шторма для интерфейса.

По умолчанию 5

Формат storm-control unicast level *0-100*

Режим Global Config

Interface Config

no storm-control unicast level

Данная команда возвращает значение порога обнаружения после одноадресного шторма на значения по умолчанию для всех интерфейсов (в режиме Global Config) либо для одного или нескольких интерфейсов (в режиме Interface Config). Функция обнаружения одноадресного шторма отключается.

Формат no storm-control unicast level

Режим Global Config

Interface Config

storm-control unicast rate

Данная команда позволяет настроить порог обнаружения одноадресного шторма на всех интерфейсах (в режиме Global Config) либо на одном или нескольких интерфейсах (в режиме Interface Config), в пакетах в секунду (pps). При включенной функции подавления одноадресных штормов трафик отбрасывается при превышении указанного порога входящим неизвестным одноадресным трафиком уровня 2 OSI. Таким образом, значение порога регулирует входящий неизвестный одноадресный трафик.

По умолчанию 0

Формат storm-control unicast rate *0*-14880000

Режим Global Config

Interface Config

no storm-control unicast rate

Данная команда возвращает значение порога обнаружения одноадресного шторма на значения по умолчанию для всех интерфейсов (в режиме Global Config) либо для одного или нескольких интерфейсов (в режиме Interface Config). Функция обнаружения одноадресного шторма отключается.

Формат no storm-control unicast rate

Режим Global Config

Interface Config

show storm-control

Данная команда предоставляет информацию о настройках коммутатора. Если вы не используете какие-либо дополнительные параметры, эта команда отображает параметры конфигурации касающиеся глобальных параметров storm-control:

- Broadcast Storm Recovery Mode может быть включен или выключен. По умолчанию - выключен.
- 802.3x Flow Control Mode может быть включен или выключен. По умолчанию - выключен.

Ключевое слово all позволяет отобразить параметры для всех интерфейсов, порт за портом. Вместо этого вы можете указать конкретный интерфейс (*unit/slot/port)* и ознакомиться с настройками именно для него.

Формат show storm-control [all | *unit/slot/port*]

Режим Privileged EXEC

Параметр	Значение
Bcast Mode	Показывает, включен ли режим контроля широковещательного шторма. По умолчанию - выключен.
Bcast Level	Уровень контроля широковещательного шторма.
Mcast Mode	Показывает, включен ли режим контроля многоадресного шторма.
Mcast Level	Уровень контроля многоадресного шторма.
Ucast Mode	Показывает, включен ли режим контроля одноадресного шторма и DLF (Destination Lookup Failure).
Ucast Level	Уровень контроля многоадресного шторма и DLF (Destination Lookup Failure).

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show storm-control
Broadcast Storm Control Mode..... Disable
Broadcast Storm Control Level..... 5 percent
```

Broadcast Storm Control Action ..... None
Multicast Storm Control Mode ..... Disable
Multicast Storm Control Level ..... 5 percent
Multicast Storm Control Action ..... None
Unicast Storm Control Mode ..... Disable
Unicast Storm Control Level ..... 5 percent
Unicast Storm Control Action..... None

ПРИМЕР: Вывод командной строки для данной команды.

(Routing) #show storm-control 1/0/1

Intf	Bcast Mode	Bcast Level	Bcast Action	Mcast Mode	Mcast Level	Mcast Action	Ucast Mode	Ucast Level	Ucast Action
1/0/1	Disable	5%	None	Disable	5%	None	Disable	5%	None

ПРИМЕР: Вывод командной строки для данной команды (частично).

(Routing) #show storm-control all

Intf	Bcast Mode	Bcast Level	Bcast Action	Mcast Mode	Mcast Level	Mcast Action	Ucast Mode	Ucast Level	Ucast Action
1/0/1	Enable	50	Trap	Disable	5%	None	Disable	5%	None
1/0/2	Enable	50	Trap	Disable	5%	None	Disable	5%	None
1/0/3	Enable	50	Trap	Disable	5%	None	Disable	5%	None
1/0/4	Enable	50	Trap	Disable	5%	None	Disable	5%	None
1/0/5	Enable	50	Trap	Disable	5%	None	Disable	5%	None
1/0/6	Enable	50	Trap	Disable	5%	None	Disable	5%	None
1/0/7	Enable	50	Trap	Disable	5%	None	Disable	5%	None
1/0/8	Enable	50	Trap	Disable	5%	None	Disable	5%	None
1/0/9	Enable	50	Trap	Disable	5%	None	Disable	5%	None
1/0/10	Enable	50	Trap	Disable	5%	None	Disable	5%	None
1/0/11	Enable	50	Trap	Disable	5%	None	Disable	5%	None
1/0/12	Enable	50	Trap	Disable	5%	None	Disable	5%	None
1/0/13	Enable	50	Trap	Disable	5%	None	Disable	5%	None
1/0/14	Enable	50	Trap	Disable	5%	None	Disable	5%	None
1/0/15	Enable	50	Trap	Disable	5%	None	Disable	5%	None
1/0/16	Enable	50	Trap	Disable	5%	None	Disable	5%	None

1/0/17	Enable	50	Trap	Disable	5%	None	Disable	5%	None
1/0/18	Enable	50	Trap	Disable	5%	None	Disable	5%	None
1/0/19	Enable	50	Trap	Disable	5%	None	Disable	5%	None

7.15. Команды Link Dependency

Следующие команды позволяют настроить функцию link dependency. Link dependency позволяет реализовать зависимость состояния линка указанных портов от состояния линка других портов. Таким образом, если на порте, от которого зависят другие порты, пропадает линк, то зависимые порты административно отключаются (и, соответственно, включаются при появлении линка на порте, от которого они зависят).

no link state track

Данная команда удаляет настройки зависимости link-dependency из группы с указанным идентификатором.

Формат no link state track *group-id*

Режим Global Config

link state group

Используйте эту команду, чтобы указать, должны ли нисходящие интерфейсы группы принимать состояние восходящих интерфейсов или инвертировать его. Согласно настройкам по умолчанию, группа имеет опцию «down» (нисходящие интерфейсы будут отражать статус восходящих, то есть при потере линка на восходящих интерфейсах отключаются и зависимые). Опция «up», напротив, включает засисимые интерфейсы при падении линка на восходящих.

По умолчанию Down

Формат link state group *group-id* action {up | down}

Режим Global Config

no link state group

Данная команда восстанавливает настройки группы на значения по умолчанию («down»).

Формат no link state group *group-id*

Режим Global Config

link state group downstream

Данная команда добавляет интерфейсы к списку нисходящих интерфейсов. После добавления интерфейса в список он отключается до тех пор, пока в группу не добавляется восходящий интерфейс. После этого статус канала начинает зависеть от интерфейса, заданного командой «upstream». Чтобы избежать отключения интерфейсов, сначала добавьте восходящий интерфейс, и лишь затем - зависимые от него интерфейсы.

Формат link state group *group-id* downstream

Режим Interface Config

no link state group downstream

Данная команда удаляет интерфейс из списка нисходящих интерфейсов.

Формат no link state group *group-id* downstream

Режим Interface Config

link state group upstream

Данная команда добавляет интерфейсы к списку восходящих интерфейсов. Обратите внимание, что интерфейс, который определен как восходящий интерфейс, не может быть одновременно определен и как нисходящий интерфейс в той же или другой группе. Создание состояния замкнутой взаимной зависимости не допускается.

Формат link state group *group-id* upstream

Режим Interface Config

no link state group upstream

Данная команда удаляет интерфейс из списка восходящих интерфейсов.

Формат no link state group *group-id* upstream

Режим Interface Config

show link state group

Данная команда отображает информацию обо всех группах Link dependency либо об указанной группе.

Формат show link state group *group-id*

Режим Privileged EXEC

ПРИМЕР: Вывод информации о всех настроенных группах.

```
(Switching)#show link-state group
```

GroupId	Downstream Interfaces	Upstream Interfaces	Link Action	Group State
1	2/0/3-2/0/7,2/0/12-2/0/17	2/0/12-2/0/32,0/3/5	Link Up	Up
4	2/0/18,2/0/27	2/0/22-2/0/33,0/3/1	Link Up	Down

ПРИМЕР: Вывод информации о указанной настроенной группе.

```
(Switching)#show link state group 1
```

GroupId	Downstream Interfaces	Upstream Interfaces	Link Action	Group State
1	2/0/3-2/0/7,2/0/12-2/0/17	2/0/12-2/0/32,0/3/5	Link Up	Up

show link state group detail

Данная команда отображает детальную информацию обо всех восходящих и нисходящих интерфейсах в пределах выбранной группы Link dependency. «Group Transitions» - это количества раз, когда нисходящий интерфейс изменил своё состояние в результате изменения состояния восходящего интерфейса.

Формат show link state group *group-id* detail

Режим Privileged EXEC

(Switching) # show link state group 1 detail

GroupId: 1

Link Action: Up

Group State: Up

Downstream Interface State:

Link Up: 2/0/3

Link Down: 2/0/4-2/0/7,2/0/12-2/0/17

Upstream Interface State:

Link Up: -

Link Down: 2/0/12-2/0/32,0/3/5

Group Transitions: 0

Last Transition Time: 00:52:35 (UTC+0:00) Jan 1 1970

7.16. Команды Port-Channel/LAG (802.3ad)

В этом разделе описываются команды, используемые для настройки port-channel, определенных в спецификации 802.3ad, и которые также известны как группы агрегации каналов (LAG). Агрегация каналов позволяет объединить несколько полнодуплексных Ethernet-соединений в единый логический канал. Сетевые устройства используют LAG как если бы это был традиционный единичный канал, что увеличивает отказоустойчивость и обеспечивает распределение нагрузки сети. Функция LAG первоначально распределяет нагрузку на основе MAC-адресов источника и получателя. После создания агрегированного канала (LAG) назначьте его членство в сети VLAN. Если этого не сделать, агрегированный канал может стать членом управляющей VLAN, что может привести к проблемам с обучением и коммутацией.

Интерфейс агрегированного канала (LAG) может быть либо статическим, либо динамическим (но не тем и другим одновременно). Все члены агрегированного канала должны использовать одни и те же протоколы. Статический интерфейс агрегированного канала не требует, чтобы партнерская система могла агрегировать свои порты-члены.

ПРИМЕЧАНИЕ: Вы можете настроить максимальное количество динамических агрегированных каналов (LAG), поддерживаемых вашей платформой. В таком случае следующие при превышения этого количества все новые агрегированные каналы будут автоматически настроены как статические.

port-channel

Данная команда создаёт и настраивает новый агрегированный канал (LAG), а также генерирует номер **unit/slot/port** для агрегированного канала. Поле name - это строка символов (допускаются буквы, цифры и дефис “-”). Команда **show port-channel all** отображает номер **unit/slot/port** для логического интерфейса. Для указания интерфейса LAG вместо **unit/slot/port** можно использовать **lag-intf-num**. Также для определения интерфейса LAG можно использовать lag **lag-intf-num**, где **lag-intf-num** - номер порта LAG.

ПРИМЕЧАНИЕ: Перед включением порта в агрегированный канал настройте физический режим порта. Для получения дополнительной информации см. "speed".

Формат port-channel name {logical-unit/slot/port | lag lag-group-id} name

Режим Global Config

addport

Данная команда добавляет один порт к port-channel (LAG). Первый интерфейс - это логический номер **unit/slot/port** настроенного агрегированного канала. В режиме Interface Config вы можете задать диапазон портов (например interface 1/0/1-1/0/4. Для указания интерфейса LAG вместо **unit/slot/port** можно использовать **lag-intf-num**. Также для определения интефейса LAG можно использовать lag **lag-intf-num**, где **lag-intf-num** - номер порта LAG.

ПРИМЕЧАНИЕ: Перед включением порта в агрегированный канал настройте физический режим порта. Для получения дополнительной информации см. "speed".

Формат addport logical unit/slot/port

Режим Interface Config

deleteport (Interface Config)

Данная команда удаляет порт или диапазон портов из агрегированного канала (LAG). Интерфейс - это логический номер **unit/slot/port** настроенного агрегированного канала (либо диапазона нескольких агрегированных каналов). Для указания интерфейса LAG вместо **unit/slot/port** можно использовать **lag-intf-num**. Также для определения интерфейса LAG можно использовать lag **lag-intf-num** - номер порта LAG.

Формат deleteport logical unit/slot/port

Режим Interface Config

deleteport (Global Config)

Данная команда удаляет все настроенные порты из агрегированного канала (LAG). Интерфейс - это логический номер *unit/slot/port* настроенного агрегированного канала. Для указания интерфейса LAG вместо **unit/slot/port** можно использовать **lag-intf-num**. Также для определения интефейса LAG можно использовать lag **lag-intf-num**, где **lag-intf-num** - номер порта LAG.

Формат deleteport logical unit/slot/port all

Режим Global Config

lacp admin key

Данная команда используется для настройки административного значения ключа для агрегированного канала. Диапазон значений: 0 – 65535. Команда может использоваться для настройки как одного интерфейса, так и диапазона интерфейсов.

По умолчанию 0x8000

Формат lacp admin key *key*

Режим Interface Config

ПРИМЕЧАНИЕ: Данная команда применима только для интерфейсов агрегированных каналов.

no lacp admin key

Данная команда используется для сброса административного значения ключа для агрегированного канала на значение по умолчанию.

Формат no lacp admin key

Режим Interface Config

lacp collector max-delay

Данная команда используется для настройки максимальной задержки коллектора агрегированного канала. Команда может использоваться для настройки как одного интерфейса, так и диапазона интерфейсов. Допустимый диапазон задержки: 0 – 65535.

По умолчанию 0x8000

Формат lacp collector max delay *delay*

Режим Interface Config

ПРИМЕЧАНИЕ: Данная команда применима только для интерфейсов агрегированных каналов.

no lacp collector max-delay

Данная команда используется для настройки максимальной задержки для агрегированного канала по умолчанию.

Формат no lacp collector max delay

Режим Interface Config

lacp actor admin key

Данная команда используется для настройки административного значения ключа действующего объекта LACP на интерфейсе или диапазоне интерфейсов. Диапазон значений: 0 – 65535.

По умолчанию Внутренний номер интерфейса данного физического порта

Формат lacp actor admin key key

Режим Interface Config

ПРИМЕЧАНИЕ: Данная команда применима только для физических интерфейсов.

no lacp actor admin key

Данная команда используется для настройки административного значения ключа по умолчанию.

Формат no lacp actor admin key

Режим Interface Config

lacp actor admin state individual

Данная команда используется для настройки административного состояния действующего объекта LACP на individual.

Формат lacp actor admin state individual

Режим Interface Config

ПРИМЕЧАНИЕ: Данная команда применима только для физических интерфейсов.

no lacp actor admin state individual

Данная команда используется для настройки административного состояния действующего объекта LACP на aggregation.

Формат lacp actor admin state individual

Режим Interface Config

lacp actor admin state longtimeout

Данная команда используется для настройки административного состояния действующего объекта LACP на longtimeout.

Формат lacp actor admin state longtimeout

Режим Interface Config

ПРИМЕЧАНИЕ: Данная команда применима только для физических интерфейсов.

no lacp actor admin state longtimeout

Данная команда используется для настройки административного состояния действующего объекта LACP на short timeout.

Формат no lacp actor admin state longtimeout

Режим Interface Config

ПРИМЕЧАНИЕ: Данная команда применима только для физических интерфейсов.

lacp actor admin state passive

Данная команда используется для настройки административного состояния действующего объекта LACP на passive.

Формат lacp actor admin state passive

Режим Interface Config

ПРИМЕЧАНИЕ: Данная команда применима только для физических интерфейсов.

no lacp actor admin state passive

Данная команда используется для настройки административного состояния действующего объекта LACP на active.

Формат no lacp actor admin state passive

Режим Interface Config

lacp actor admin state

Данная команда используется для настройки административного значения состояния действующего объекта согласно передаваемому значению действующим объектом в LACPDU. Команда может использоваться для настройки как одного интерфейса, так и диапазона интерфейсов.

По умолчанию 0x07

Формат lacp actor admin state {individual|longtimeout|passive}

Режим Interface Config

ПРИМЕЧАНИЕ: Данная команда применима только для физических интерфейсов.

no lacp actor admin state

Данная команда используется для настройки административных значений действующего объекта по умолчанию, согласно передаваемому значению действующим объектом в LACPDU.

ПРИМЕЧАНИЕ: Обе команды: **no portlacptimeout** и **no lacp actor admin state** - настраивают значения на настройки по умолчанию, несмотря на команды, используемые для настройки портов. Таким образом, обе команды будут отображаться в **show running-config**.

Формат no lacp actor admin state {individual|longtimeout|passive}

Режим Interface Config

lacp actor port priority

Данная команда используется для настройки значения приоритета, назначенного интерфейсу или группе интерфейсов Aggregation Port. Диапазон значений - от 0 до 65535.

По умолчанию 0x80

Формат lacp actor port priority *0-65535*

Режим Interface Config

ПРИМЕЧАНИЕ: Данная команда применима только для физических интерфейсов.

no lacp actor port priority

Данная команда используется для установки значения приоритета, назначенного интерфейсу или группе интерфейсов Aggregation Port, на значения по умолчанию.

Формат no lacp actor port priority

Режим Interface Config

lacp partner admin key

Данная команда используется для настройки административного значения ключа для партнера. Команда может использоваться для настройки как одного интерфейса, так и диапазона интерфейсов. Диапазон значений - от 0 до 65535.

По умолчанию 0x0

Формат lacp partner admin key *key*

Режим Interface Config

ПРИМЕЧАНИЕ: Данная команда применима только для физических интерфейсов.

no lacp partner admin key

Данная команда используется для сброса административного значения ключа для партнера на значения по умолчанию.

Формат no lacp partner admin key

Режим Interface Config

lacp partner admin state individual

Данная команда используется для настройки административного состояние партнера LACP на individual.

Формат lacp partner admin state individual

Режим Interface Config

ПРИМЕЧАНИЕ: Данная команда применима только для физических интерфейсов.

no lacp partner admin state individual

Данная команда используется для настройки административного состояние партнера LACP на aggregation.

Формат no lacp partner admin state individual

Режим Interface Config

lacp partner admin state longtimeout

Данная команда используется для настройки административного состояние партнера LACP на longtimeout.

Формат lacp partner admin state longtimeout

Режим Interface Config

ПРИМЕЧАНИЕ: Данная команда применима только для физических интерфейсов.

no lacp partner admin state longtimeout

Данная команда используется для настройки административного состояние партнера LACP на short timeout.

Формат no lacp partner admin state longtimeout

Режим Interface Config

ПРИМЕЧАНИЕ: Данная команда применима только для физических интерфейсов.

lacp partner admin state passive

Данная команда используется для настройки административного состояние партнера LACP на passive.

Формат lacp partner admin state passive

Режим Interface Config

ПРИМЕЧАНИЕ: Данная команда применима только для физических интерфейсов.

no lacp partner admin state passive

Данная команда используется для настройки административного состояние партнера LACP на active.

Формат no lacp partner admin state passive

Режим Interface Config

lacp partner port id

Данная команда настраивает идентификатор партнера LACP. Команда может использоваться для настройки как одного интерфейса, так и диапазона интерфейсов. Диапазон значений - от 0 до 65535.

По умолчанию 0x80

Формат lacp partner port-id port-id

Режим Interface Config

ПРИМЕЧАНИЕ: Данная команда применима только для физических интерфейсов.

lacp partner port id

Данная команда используется для сброса административного состояние партнера LACP на значения по умолчанию.

Формат no lacp partner port-id

Режим Interface Config

lacp partner port priority

Данная команда используется для настройки приоритета порта партнера LACP. Команда может использоваться для настройки как одного интерфейса, так и диапазона интерфейсов. Диапазон значений - от 0 до 65535.

По умолчанию 0x0

Формат lacp partner port priority *priority*

Режим Interface Config

ПРИМЕЧАНИЕ: Данная команда применима только для физических интерфейсов.

no lacp partner port priority

Данная команда используется для сброса приоритета порта партнера LACP на значения по умолчанию.

Формат no lacp partner port priority

Режим Interface Config

lacp partner system id

Данная команда настраивает значение MAC-адреса (6 октетов), отражающее административное значение System ID партнера протокола аггрегации. Команда может использоваться для настройки как одного интерфейса, так и диапазона интерфейсов. Допустимый диапазон *system-id*: 00:00:00:00:00:00 – FF:FF:FF:FF:FF.

По умолчанию 00:00:00:00:00:00

Формат lacp partner system-id *system-id*

Режим Interface Config

ПРИМЕЧАНИЕ: Данная команда применима только для физических интерфейсов.

no lacp partner system-id

Данная команда устанавливает значение по умолчанию, отражающее административное значение System ID партнера протокола аггрегации.

Формат no lacp partner system-id

Режим Interface Config

lacp partner system priority

Данная команда устанавливает значение приоритета, ассоциированного с System ID партнера. Команда может использоваться для настройки как одного интерфейса, так и диапазона интерфейсов. Диапазон значений - от 0 до 65535.

По умолчанию 0x0

Формат lacp partner system priority *0-65535*

Режим Interface Config

ПРИМЕЧАНИЕ: Данная команда применима только для физических интерфейсов.

no lacp partner system priority

Данная команда сбрасывает значение приоритета, ассоциированного с System ID партнера, на значение по умолчанию.

Формат no lacp partner system priority

Режим Interface Config

interface lag

Данная команда используется для входа в режим настройки интерфейса для указанного LAG.

Формат interface lag *lag-interface-number*

Режим Global Config

port-channel static

Данная команда активирует статический режим на интерфейсе агрегированного канала (LAG) или диапазоне таких интерфейсов. По умолчанию для нового агрегированного канала применяется именно статический режим. Если в системе уже присутствует максимально разрешенное количество динамических агрегированных каналов, для новых агрегированных каналов доступен только статический режим. Данная команда применима только для интерфейсов агрегированных каналов.

По умолчанию включено

Формат port-channel static

Режим Interface Config

no port-channel static

Данная команда позволяет настроить динамический режим на определенном интерфейсе агрегированного канала (LAG). Данная команда применима только для интерфейсов агрегированных каналов.

Формат no port-channel static

Режим Interface Config

port lacpmode

Данная команда активирует протокол LACP (Link Aggregation Control Protocol) на порте либо на диапазоне портов.

По умолчанию включено

Формат port lacpmode

Режим Interface Config

no port lacpmode

Данная команда отключает протокол LACP (Link Aggregation Control Protocol) на порте.

Формат no port lacpmode

Режим Interface Config

port lacpmode enable all

Данная команда активирует протокол LACP (Link Aggregation Control Protocol) на всех портах.

Формат port lacpmode enable all

Режим Global Config

no port lacpmode enable all

Данная команда отключает протокол LACP (Link Aggregation Control Protocol) на всех портах.

Формат no port lacpmode enable all

Режим Global Config

port lacptimeout (Interface Config)

Данная команда настраивает таймаут на физическом интерфейсе или на диапазоне интерфейсов определенного типа устройств (действующий объект либо партнер). Возможные значения: long (длинный) или short (короткий).

По умолчанию long

Формат port lacptimeout {actor | partner} {long | short}

Режим Interface Config

no port lacptimeout

Данная команда возвращает значение таймаута по умолчанию.

Формат no port lacptimeout {actor | partner}

Режим Interface Config

ПРИМЕЧАНИЕ: Обе команды: **no port lacptimeout** и **no lacp actor admin state** - настраивают значения на настройки по умолчанию, несмотря на команды, используемые для настройки портов. Таким образом, обе команды будут отображаться в **show running-config**.

port lacptimeout (Global Config)

Данная команда настраивает таймаут для всех интерфейсов определенного типа устройств (действующий объект либо партнер). Возможные значения: long (длинный) или short (короткий).

По умолчанию long

Формат port lacptimeout {actor | partner} {long | short}

Режим Global Config

no port lacptimeout

Данная команда настраивает таймаут для всех физических интерфейсов определенного типа устройств (действующий объект либо партнер) на заводские значения.

Формат no port lacptimeout {actor | partner}

Режим Global Config

ПРИМЕЧАНИЕ: Обе команды: **no port lacptimeout** и **no lacp actor admin state** - настраивают значения на настройки по умолчанию, несмотря на команды, используемые для настройки портов. Таким образом, обе команды будут отображаться в **show running-config**.

port-channel adminmode

Данная команда включает все настроенные агрегированные каналы с тем же административным режимом.

Формат port-channel adminmode all

Режим Global Config

no port-channel adminmode

Данная команда отключает все настроенные агрегированные каналы с тем же административным режимом.

Формат no port-channel adminmode all

Режим Global Config

port-channel linktrap

Данная команда активирует уведомления link trap для агрегированного канала (LAG). Интерфейс - это логический номер *unit/slot/port* настроенного агрегированного канала. Опция all настраивает каждый настроенный агрегированный канал с тем же административным режимом. Для указания интерфейса LAG вместо *unit/slot/port* можно использовать lag-intf-num. Также для определения интерфейса LAG можно использовать lag *lag-intf-num*, где *lag-intf-num* - номер порта LAG.

По умолчанию включено

Формат port-channel linktrap {*logical unit/slot/port* | all}

Режим Global Config

no port-channel linktrap

Данная команда отключает уведомления link trap для агрегированного канала (LAG). Интерфейс - это логический слот и порт для настроенного агрегированного канала. Опция all настраивает каждый настроенный агрегированный канал с тем же административным режимом.

Формат no port-channel linktrap {*logical unit/slot/port* | all}

Режим Global Config

port-channel load-balance

Эта команда выбирает параметр балансировки нагрузки, используемый на агрегированном канале (LAG). Балансировка трафика происходит на агрегированном канале (LAG) путем выбора одного из линков в канале для передачи конкретных пакетов. Соединение выбирается путем создания двоичного шаблона из выбранных полей в пакете и связывания этого шаблона с конкретным линком.

Балансировка нагрузки поддерживается не всеми устройствами. Набор опций балансировки нагрузки может также отличаться на разных устройствах.

Команду можно применить для одного интерфейса, диапазона интерфейсов либо для всех интерфейсов. Для указания интерфейса LAG вместо **unit/slot/port** можно использовать **lag-intf-num**. Также для определения интерфейса LAG можно использовать lag **lag-intf-num, где lag-intf-num** - номер порта LAG.

По умолчанию 3

Форма port-channel load-balance {1 | 2 | 3 | 4 | 5 | 6 | 7} {*unit/slot/port* | all}

Режим Interface Config

Global Config

Термин	Значение
1	MAC-адрес источника, VLAN, тип Ethernet и входящий порт пакета.
2	MAC-адрес назначения, VLAN, тип Ethernet и входящий порт, пакета.
3	MAC-адрес назначения/источника, VLAN, тип Ethernet и входящий порт пакета.
4	Поля пакета: IP-адрес источника и TCP/UDP источника
5	Поля пакета: IP-адрес назначения и TCP/UDP-порт назначения
6	Поля пакета: IP-адреса назначения/источника и TCP/UDP-порт назначения/источника
7	Режим улучшенного хеширования.
unit/slot/port| all	Только режим Config Mode: Интерфейс - это логический номер unit/slot/port настроенного агрегированного канала. All - применить ко всем агрегированным каналам, настроенным в настоящий момент.

no port-channel load-balance

Данная команда возвращает для балансировки нагрузки конфигурацию по умолчанию.

Формат no port-channel load-balance {*unit/slot/port* | all}

Режим Interface Config

Global Config

port-channel local-preference

Данная команда активирует режим локального предпочтения на интерфейсе агрегированного канала (LAG) или диапазоне таких интерфейсов. По умолчанию режим локального предпочтения для агрегированного канала отключен. Данная команда применима только для интерфейсов агрегированных каналов.

По умолчанию отключено

Формат port-channel local-preference

Режим Interface Config

no port-channel local-preference

Данная команда отключает режим локального предпочтения на интерфейсе агрегированного канала (LAG).

Формат no port-channel local-preference

Режим Interface Config

port-channel min-links

Данная команда позволяет настроить минимальное количество каналов для интерфейсов LAG.

По умолчанию 1

Формат port-channel min-links *1-8*

Режим Interface Config

port-channel name

Данная команда позволяет настроить имя для агрегированного канала (LAG). Интерфейс - это логический **unit/slot/port** для настроенного агрегированного канала, а **name** – это строка из букв и цифр (до 15 символов). Для указания интерфейса LAG вместо **unit/slot/port** можно использовать **lag-intf-num**. Также для определения интерфейса LAG можно использовать lag **lag-intf-num** - номер порта LAG.

Формат port-channel name {*logical unit/slot/port*} *name*

Режим Global Config

port-channel system priority

Данная команда используется для настройки системного приоритета агрегированного канала. Диапазон значений: 0 – 65535.

По умолчанию 0x8000

Формат port-channel system priority *priority*

Режим Global Config

no port-channel system priority

Данная команда используется для установки значений по умолчанию для системного приоритета агрегированного канала.

Формат no port-channel system priority

Режим Global Config

show lacp actor

Данная команда отображает атрибуты действующего объекта LACP. Для указания интерфейса LAG вместо **unit/slot/port** можно использовать **lag-intf-num**. Также для определения интерфейса LAG можно использовать lag **lag-intf-num**, где **lag-intf-num** - номер порта LAG.

Формат show lacp actor {*unit/slot/port*|all}

Режим Global Config

Вывод команды содержит следующие параметры.

Параметр	Описание
System Priority	Административное значение Ключа.
Actor Admin Key	Административное значение Ключа.
Port Priority	Значение приоритета, назначенное агрегированному порту.
Admin State	Административное значение действующего объекта согласно передаваемому значению действующим объектом в LACPDU.

show lacp partner

Данная команда отображает атрибуты партнера LACP. Для указания интерфейса LAG вместо **unit/slot/port** можно использовать **lag-intf-num**. Также для определения интерфейса LAG можно использовать **lag lag-intf-num**, где **lag-intf-num** - номер порта LAG.

Формат show lacp actor {*unit/slot/port*|all}

Режим Privileged EXEC

Вывод команды содержит следующие параметры.

Параметр	Описание
System Priority	Административное значение приоритета, ассоциированного с System ID партнера.
System-ID	Административное значение System ID партнера протокола Aggregation Port.
Admin Key	Административное значение ключа для партнера протокола.
Port Priority	Административное значение ключа для партнера протокола.
Port-ID	Административное значение номера порта для партнера протокола.
Admin State	Административные значения состояние действующего объекта для партнера протокола.

show port-channel brief

Данная команда отображает статические возможности всех интерфейсов агрегированного канала (LAG) на устройстве, а также сводную информацию об индивидуальных интерфейсах агрегированного канала. Для указания интерфейса LAG вместо **unit/slot/port** можно использовать **lag-intf-num**. Также для определения интерфейса LAG можно использовать lag **lag-intf-num**, где **lag-intf-num** - номер порта LAG.

Формат show port-channel brief

Режим User EXEC

Для каждого агрегированного канала отображается следующая информация:

Термин	Значение
Logical Interface	Unit/slot/port логического интерфейса.
Port-channel Name	Имя интерфейса агрегированного канала (LAG).
Link-State	Состояние линка up или down.
Trap Flag	Информация о том, включены ли trap или нет.
Термин	Значение
Type	Информация о типе аггрегированного канала, статический или динамический.
Mbr Ports	Члены агрегированного канала.
Active Ports	Порты, активно участвующие в агрегированном канале.

show port-channel

Данная команда предоставляет обзор всех агрегированных каналов (LAG) на коммутаторе. Для указания интерфейса LAG вместо *unit/slot/port* можно использовать *lag-intf-num*. Также для определения интерфейса LAG можно использовать lag *lag-intf-num*, где *lag-intf-num* - номер порта LAG.

Формат show port-channel

Режимы Privileged EXEC

Термин	Значение
Logical Interface	Действительный номер unit/slot/port.
Port-Channel Name	Имя данного агрегированного канала (LAG). Строка из цифр и букв (до 15 символов).

Термин	Значение
Link State	Состояние линка up или down.
Admin Mode	Может быть включенным или отключенным. По умолчанию - включено.
Type	Информация о типе аггрегированного канала, статический или динамический.
Load Balance Option	Настройки балансировки нагрузки, ассоциированные с этим LAG. См. “port-channel load-balance”.
Local Preference Mode	Указывает на состояние режима локального предпочтения: включен ли он (enabled) или выключен (disabled).
Mbr Ports	Список портов-членов данного агрегированного канала (LAG). Агрегированному каналу может быть назначено до 8 портов.
Device Timeout	Для каждого порта указан таймаут (long или short) для типа устройства (actor или partner).
Port Speed	Скорость порта агрегированного канала.
Active Ports	В этом поле перечисляются порты, активно участвующие в агрегированном канале (LAG).

ПРИМЕР: Вывод командной строки для данной команды.

```
(Switch) #show port-channel 0/3/1
Local Interface.....0/3/1
Channel Name .....ch1
Link State.....Up
Admin Mode.....Enabled
Type.....Static
Load Balance Option .....3
(Src/Dest MAC, VLAN, EType, incoming port)
Local Preference Mode.....Enabled
Mbr Ports       Device/Timeout                 Port Speed      Port Active
------ ------------ --------- ------------------------------------------------------
1/0/1           actor/long      Auto          True            partner/long
1/0/2           actor/long      Auto          True            partner/long
1/0/3           actor/long      Auto          False           partner/long
```

1/0/4	actor/long	Auto	False	partner/long

show port-channel system priority

Данная команда используется для отображения настроек системного приоритета агрегированного канала.

Формат show port-channel system priority

Режим Privileged EXEC

show port-channel counters

Данная команда отображает счетчики для указанного порта агрегированного канала.

Формат show port-channel *unit/slot/port* counters

Режим Privileged EXEC

Термин	Значение
Local Interface	Действительный номер slot/port.
Channel Name	Имя данного агрегированного канала (LAG).
Link State	Состояние линка up или down.
Admin Mode	Может быть включенным или отключенным. По умолчанию - включено.
Port Channel Flap Count	Количество периодов неактивности агрегированного канала.
Mbr Ports	Члены аггрегированного канала.
Mbr Flap Counters	Количество периодов неактивности агрегированного канала, произошедших по причине отсутствия линка либо административного отключения.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Switch) #show port-channel 3/1 counters
Local Interface.....3/1
Channel Name .....ch1
Link State.....Down
Admin Mode.....Enabled
Port Channel Flap Count .....0
```

Mbr Ports	Mbr Flap Counters
0/1	0
0/2	0
0/3	1
0/4	0
0/5	0
0/6	0
0/7	0
0/8	0

clear port-channel counters

Данная команда очищает и сбрасывает счётчики flap counters для указанного интерфейса.

Формат clear port-channel {lag-intf-num | unit/slot/port} counters

Режим Privileged EXEC

clear port-channel all counters

Данная команда очищает и сбрасывает все счётчики flap counters для указанного интерфейса.

Формат clear port-channel all counters

Режим Privileged EXEC

7.17. Команды зеркалирования портов

Зеркалирование портов (также известное как мониторинг порта) выбирает сетевой трафик, который вы можете анализировать с помощью сетевого анализатора, такого как устройство SwitchProbe. Также вы можете использовать другое решение для удаленного мониторинга (RMON).

monitor session source

Данная команда позволяет сконфигурировать интерфейс-источник для выбранного сеанса мониторинга. Для указания конкретного интерфейса для мониторинга используйте параметр **source interface unit/ slot/port**. Параметр **rx** активирует мониторинг исключительно входящих пакетов, а параметр **tx** – только исходящих. Если опция **{rx | tx}** не указана, будет производиться мониторинг как для входящих, так и для исходящих пакетов. Параметр session-id представляет собой целочисленное значение, используемое для идентификации сеанса.

В качестве интерфейса-источника можно указать VLAN, тогда в данной сессии будет производиться мониторинг всех портов данной VLAN.

ПРИМЕЧАНИЕ: Если интерфейс участвует в некоей VLAN и является членом LAG, эта VLAN не может быть назначена в качестве VLAN-источника для сеанса мониторинга. В то же время, если интерфейс участвует в некоей VLAN, и эта VLAN назначается в качестве VLAN-источника для сеанса мониторинга, интерфейс может быть назначен как член LAG.

Удаленное зеркалирование портов настраивается добавлением RSPAN VLAN ID. На коммутаторе источника RSPAN VLAN указывается в качестве назначения, а на коммутаторе назначения, соответственно, RSPAN VLAN укзаывается в качестве источника.

ПРИМЕЧАНИЕ: Источник и получатель не могут быть настроены как удаленные на одном устройстве.

ПРИМЕЧАНИЕ: На промежуточном коммутаторе должна быть создана RSPAN VLAN, порты, подключенные к коммутаторам источника и назначения, должны быть членами в данной VLAN RSPAN. На интерфейсе промежуточного коммутатора, подключенного к коммутатору назначения, должно быть включено выходное тегирование RSPAN VLAN.

По умолчанию	Нет
Формат	monitor session session-id source {interface {unit/slot/port | cpu | lag } | vlan vlanid | remote vlan vlan-id }[{rx | tx}]
Режим	Global Config

no monitor session source

Данная команда удаляет указанный зеркалированный порт из сеанса мониторинга.

По умолчанию	Нет
Формат	no monitor session session-id source {interface {unit/slot/port | cpu | lag } | vlan | remote vlan}
Режим	Global Config

monitor session destination

Данная команда позволяет настроить интерфейс получатель для выбранного сеанса мониторинга. Команда настраивает порт получатель для выбранного сеанса мониторинга.

Порт reflector-port настраивается на коммутаторе-источнике вместе с RSPAN VLAN назначения. Порт reflectorport перенаправляет зеркалируемый трафик на коммутатор назначения.

ПРИМЕЧАНИЕ: Этот порт должен быть настроен с членством в RSPAN VLAN.

Параметр destination interface unit/slot/port позволяет указать интерфейс для приёма зеркалированного трафика.

По умолчанию	Нет
Формат	monitor session session-id destination {interface unit/slot/port |remote vlan vlanid reflector-port unit/slot/port}
Режим	Global Config

no monitor session destination

Данная команда удаляет указанный порт получатель из сеанса мониторинга.

Формат no monitor session session id destination {interface unit/slot/port |remote vlan vlanid reflector-port unit/slot/port}

Режим Global Config

monitor session filter

Данная команда прикрепляет IP/MAC ACL к выбранному сеансу мониторинга.

IP/MAC ACL может быть прикреплен к сеансу путём указания номера либо имени списка доступа.

Параметр filter фильтрует указанную группу доступа либо по IP, либо по MAC.

ПРИМЕЧАНИЕ: IP/MAC ACL может быть прикреплен к сеансу путём указания номера либо имени списка доступа. На платформах, которые не поддерживают списки управления доступом по IP и по MAC, при попытке настройки ACL обоих типов возвращается сообщение об ошибке.

По умолчанию Нет

Формат monitor session session-id filter {ip access-group acl-id/aclname | mac access-group acl-name}

Режим Global Config

no monitor session filter

Данная команда удаляет указанный IP/MAC ACL из сеанса мониторинга.

Формат no smonitor session *session-id* filter {ip access-group | mac access-group }

Режим Global Config

monitor session mode

Данная команда активирует выбранный сеанс мониторинга.

По умолчанию Нет

Формат monitor session *session-id* mode

Режим Global Config

no monitor session mode

Данная команда отключает выбранный сеанс мониторинга.

Формат no monitor session *session-id* mode

Режим Global Config

no monitor session

Используйте эту команду без дополнительных параметров, чтобы удалить сеанс мониторинга из порта источника, порта назначения мониторинга и всех VLAN. После удаления порта из VLAN, добавлять его в любую нужную VLAN необходимо вручную. Параметры **source interface unit/slot/port** или **destination interface** используются для удаления указанных интерфейсов из сеанса мониторинга порта. Параметр **mode** позволяет отключить административный режим сеанса.

Формат no monitor session *session-id* {source {interface *unit/slot/port* | cpu | lag} |vlan| remote vlan} | destination { interface | remote vlan | mode |filter {ip access-group |mac access-group}}]

Режим Global Config

no monitor

Данная команда удаляет все порты-источники и порт назначения, и восстанавливает значения по умолчанию для всех настроенных сеансов зеркалирования портов.

ПРИМЕЧАНИЕ: Это отдельная «no»-команда. «Нормальной» формы команда не имеет.

По умолчанию включено

Формат no monitor

Режим Global Config

show monitor session

Данная команда отображает информацию о мониторинге порта для конктретного сеанса мониторинга.

ПРИМЕЧАНИЕ: Параметр **session-id** – цельночисленное значение, используемое для идентификации сеанса.

Формат show monitor session *session-id*

Режим Privileged EXEC

Термин	Значение
Session ID	Цельночисленное значение, используемое для идентификации сеанса. Данное значение может принадлежать к диапазону между 1 и максимальным количеством разрешенных на платформе сеансов мониторинга.
Admin Mode	Указывает, включена или выключена функция мониторинга порта для сеанса, определяемого *session-id*. Возможные значения: Enabled (Включено) и Disabled (Отключено).
Probe Port	Порт назначения для сеанса, определяемого *session-id*. Если порт probe не настроен, это поле остается пустым.
MIrrored Port	Порт, настроенный в качестве зеркалируемого (порта источника) для сеанса, определяемого *session-id*. Если порт источника не настроен, это поле остается пустым.
Type	Направление, в котором порт источника настроен для зеркалирования портов. («tx» для переданных пакетов и «rx» – для принятых.)

ПРИМЕР 1:

```
(Switch)#show monitor session 1
```

Session ID	Admin Mode	Probe Port	Mirrored Port	Type
1	Enable	1/0/8	1/0/10	Rx,Tx

ПРИМЕР 2:

(Switch)#show monitor session all

Session ID	Admin Mode	Probe Port	Mirrored Port	Type
1	Enable	1/0/8	1/0/10	Rx,Tx
2	Disable			
3	Disable	1/0/11		
4	Enable	1/0/11	1/0/7	Tx

ПРИМЕР: 3:

(Switch)#show monitor session all

Session ID	Admin Mode	Probe Port	Mirrored Port	Type
1	Enable	1/0/8	1/0/10	Rx
2	Enable			Rx
3	Disable			Tx
4	Disable	1/0/11	1/0/7	Tx

ПРИМЕР: 4:

(Switch)#show monitor session all

Session ID	Admin Mode	Probe Port	Mirrored Port	Type
1	Enable		1/0/15	Tx
2	Enable	1/0/3	1/0/15	Tx
3	Enable		1/0/15	Rx
4	Enable	1/0/11	1/0/15	Rx

ПРИМЕР: 5:

(Switch)#show monitor session all

Session ID	Admin Mode	Probe Port	Mirrored Port	Type
1	Disable			
2	Disable			
3	Enable	1/0/16		
4	Enable	1/0/11	1/0/16	Tx, Rx

ПРИМЕР: 6:

(Switch)#show monitor session all

Session ID	Admin Mode	Probe Port	Mirrored Port	Type
1	Enable			
2	Enable	1/0/15		
3	Enable			
4	Enable	1/0/11	1/0/16	Rx, Tx

show vlan remote-span

Эта команда отображает настроенные RSPAN VLAN .

Формат show vlan remote-span

Режим Privileged EXEC

ПРИМЕР: Вывод командной строки для данной команды.

```
(Switch)# show vlan remote-span
Remote SPAN VLAN
----------------------------
100,102,201,303
```

7.18. Команды статической фильтрации MAC-адресов

В этом разделе описываются команды, применяемые для настройки статической фильтрации MAC-адресов. Статическая фильтрация MAC позволяет настраивать порты назначения для статической многоадресной фильтрации MAC, независимо от платформы.

macfilter

Данная команда добавляет запись статического фильтра MAC для MAC-адреса **macaddr** во VLAN **vlanid**. Значение параметра **macaddr** - это 6-байтовое шестнадцатеричное число в формате b1:b2:b3:b4:b5:b6. Недопустимые MAC-адреса: 00:00:00:00:00:00, диапазоны: 01:80:C2:00:00:00-01:80:C2:00:00:0F, 01:80:C2:00:00:20-01:80:C2:00:00:21, и FF:FF:FF:FF:FF:FF. Параметр **vlanid** должен соответствовать реальной VLAN.

Количество статических фильтров MAC, поддерживаемых системой, различается для тех фильтров MAC, в которых настроены порты-источники, и тех фильтров, в которых настроены порты назначения.

- Для одноадресных и многоадресных фильтров MAC-адресов со списками портов источника максимальное количество поддерживаемых статических MAC-фильтров составляет 20.
- Для многоадресных фильтров MAC-адресов с настроенными портами назначения максимальное количество поддерживаемых статических фильтров составляет 256.

Таким образом, для текущих платформ вы можете настроить следующие комбинации:

- Одноадресный MAC-адрес и порт источника (до 20)
- Многоадресный MAC-адрес и порт источника (до 20)

- Многоадресный MAC-адрес и только порт назначения (до 256)
- Многоадресные MAC-адреса и порты источника и назначения (до 20)

Формат macfilter *macaddr vlanid*

Режим Global Config

no macfilter

Данная команда удаляет все ограничения и запись статического фильтра MAC для MAC-адреса (**macaddr**) во VLAN (**vlanid**). Значение параметра **macaddr** - это 6-байтовое шестнадцатеричное число в формате b1:b2:b3:b4:b5:b6.

Параметр **vlanid** должен соответствовать реальной VLAN.

Формат no macfilter *macaddr vlanid*

Режим Global Config

macfilter adddest

Данная команда добавляет интерфейс или диапазон интерфейсов к набору фильтров назначения для фильтра MAC, с указанными MAC-адресом **macaddr** и VLAN of **vlanid**. Значение параметра **macaddr** - это 6-байтовое шестнадцатеричное число в формате b1:b2:b3:b4:b5:b6. Параметр **vlanid** должен соответствовать реальной VLAN.

ПРИМЕЧАНИЕ: Настройка порта назначения действительна только для многоадресных MAC-адресов.

Формат macfilter adddest *macaddr*

Режим Interface Config

no macfilter adddest

Данная команда удаляет порт из набора фильтров назначения для фильтра MAC, с указанными MAC-адресом (**macaddr**) и VLAN (**vlanid**).

Формат no macfilter adddest *macaddr*

Режим Interface Config

macfilter adddest all

Данная команда добавляет все интерфейсы к набору фильтров назначения для фильтра MAC, с указанными MAC-адресом (**macaddr**) и VLAN of (**vlanid**). Значение параметра *macaddr* - это 6-байтовое шестнадцатеричное число в формате b1:b2:b3:b4:b5:b6. Параметр **vlanid** должен соответствовать реальной VLAN.

ПРИМЕЧАНИЕ: Настройка порта назначения действительна только для многоадресных MAC-адресов.

Формат macfilter adddest all *macaddr*

Режим Global Config

no macfilter adddest all

Данная команда удаляет все порты из набора фильтров назначения для фильтра MAC, с указанными MAC-адресом (**macaddr**) и VLAN (**vlanid**).

Формат no macfilter adddest all *macaddr*

Режим Global Config

macfilter addsrc

Данная команда добавляет интерфейс или диапазон интерфейсов к набору фильтров источника для фильтра MAC, с указанными MAC-адресом (**macaddr**) и VLAN of (**vlanid**). Значение параметра **macaddr** - это 6-байтовое шестнадцатеричное число в формате b1:b2:b3:b4:b5:b6.

Параметр *vlanid* должен соответствовать реальной VLAN.

Формат macfilter addsrc *macaddr vlanid*

Режим Interface Config

no macfilter addsrc

Данная команда удаляет порт из набора фильтров источника для фильтра MAC, с указанными MAC-адресом (**macaddr**) и VLAN (**vlanid**).

Формат no macfilter addsrc *macaddr vlanid*

Режим Interface Config

macfilter addsrc all

Данная команда добавляет все интерфейсы к набору фильтров источника для фильтра MAC, с указанными MAC-адресом (**macaddr**) и (**vlanid**). Значение параметра **macaddr** - это 6-байтовое шестнадцатеричное число в формате b1:b2:b3:b4:b5:b6. Параметр **vlanid** должен соответствовать реальной VLAN.

Формат macfilter addsrc all *macaddr vlanid*

Режим Global Config

no macfilter addsrc all

Данная команда удаляет все интерфейсы из набора фильтров источника для фильтра MAC, с указанными MAC-адресом (**macaddr**) и (**VLAN vlanid**).

Формат no macfilter addsrc all *macaddr vlanid*

Режим Global Config

show mac-address-table static

Данная команда отображает информацию о всех статических фильтрах MAC. Опция all, отображает все статические фильтры MAC в системе. При указании значения *macaddr* необходимо также указать значение **vlanid**. В этом случае система отобразит инфомацию о статических фильтрах MAC только для указанных MAC-адреса и VLAN.

Формат show mac-address-table static {*macaddr vlanid* | all}

Режим Privileged EXEC

Термин	Значение
MAC Address	MAC-адрес записи статического фильтра MAC.
VLAN ID	VLAN ID записи статического фильтра MAC.
Source Port(s)	Порт источника набора фильтров слота и порта (портов).

ПРИМЕЧАНИЕ: Списки портов назначения имеют только многоадресные фильтры.

show mac-address-table staticfiltering

Данная команда отображает записи статической фильтрации в таблице MFDB (Multicast Forwarding Database).

Формат show mac-address-table staticfiltering

Режим Privileged EXEC

Термин	Значение
VLAN ID	VLAN, в которой изучен MAC-адрес.
MAC Address	Индивидуальный MAC-адрес, для которого коммутатор имеет информацию о перенаправлении или фильтрации. По мере сбора данных из MFDB адрес станет многоадресным. Формат - 6 двухзначных шестнадцатеричных чисел, разделенных двоеточиями, например 01:23:45:67:89:AB.
Type	Тип записи. Статические записи сгенерирвоаны конечным пользователем. Динамические – добавлены в таблицу в результате процесса обучения или протокола.
Description	Текстовое описание записи.
Interfaces	Список интерфейсов, предназначенных для перенаправления (Fwd:) и фильтрации (Flt:).

7.19. Команды конфигурации DHCP Snooping

В этом разделе описаны команды, которые используются для настройки DHCP Snooping.

ip dhcp snooping enable

Данная команда глобально включает DHCP Snooping.

По умолчанию отключено
Формат ip dhcp snooping
Режим Global Config

no ip dhcp snooping enable

Данная команда глобально отключает DHCP Snooping.

Формат no ip dhcp snooping
Режим Global Config

ip dhcp snooping vlan

Данная команда включает DHCP snooping для списка VLAN (разделяются запятыми).

По умолчанию отключено
Формат ip dhcp snooping vlan *vlan-list*
Режим Global Config

no ip dhcp snooping vlan

Данная команда отключает DHCP Snooping для VLAN.

Формат no ip dhcp snooping vlan *vlan-list*
Режим Global Config

ip dhcp snooping verify mac-address

Данная команда используется для включения функции сверки MAC-адреса источника с MAC-адресом клиента в полученных сообщениях DHCP.

По умолчанию включено
Формат ip dhcp snooping verify mac-address
Режим Global Config

no ip dhcp snooping verify mac-address

Данная команда используется для отключения функции сверки MAC-адреса источника с MAC-адресом клиента.

Формат no ip dhcp snooping verify mac-address
Режим Global Config

ip dhcp snooping database

Данная команда настраивает постоянное местоположение базы данных DHCP Snooping. Это может быть как локальный, так и удалённый файл (на устройстве с указанным IP).

По умолчанию local
Формат ip dhcp snooping database {local|tftp://hostIP/filename}
Режим Global Config

ip dhcp snooping database write-delay

Данная команда настраивает интервал (в секундах), с которым будет сохраняться база данных DHCP Snooping. Диапазон времени: 15 – 86400 секунды.

По умолчанию 300 секунд

Формат ip dhcp snooping database write-delay in seconds

Режим Global Config

no ip dhcp snooping database write-delay

Данная команда сбрасывает настройки интервала записи на значения по умолчанию.

Формат no ip dhcp snooping database write-delay

Режим Global Config

ip dhcp snooping binding

Данная команда позволяет настроить статическую привязку DHCP Snooping.

Формат ip dhcp snooping binding mac-address vlan vlan id ip address interface interface id

Режим Global Config

no ip dhcp snooping binding

Данная команда удаляет статическую запись DHCP из базы данных DHCP Snooping.

Формат no ip dhcp snooping binding *mac-address*

Режим Global Config

ip dhcp snooping limit

Данная команда используется для настройки скорости, с которой сообщения DHCP Snooping поступают на интерфейс или диапазон интерфейсов. Отключено по умолчанию. При включении скорость может быть настроена в диапазоне от 0 до 300 пакетов в секунду. Диапазон burst level: от 1 до 15 секунд.

По умолчанию отключено (без лимита)

Формат ip dhcp snooping limit {rate pps [*burst interval seconds*]}

Режим nterface Config

no ip dhcp snooping limit

Данная команда используется для сброса скорости отправки сообщений DHCP Snooping и burst level на значения по умолчанию.

Формат no ip dhcp snooping limit

Режим Interface Config

ip dhcp snooping log-invalid

Данная команда позволяет настроить логирование фильтрации DHCP-сообщений при помощи приложения DHCP Snooping. Команда может использоваться для настройки как одного интерфейса, так и диапазона интерфейсов.

По умолчанию отключено

Формат ip dhcp snooping log-invalid

Режим Interface Config

no ip dhcp snooping log-invalid

Данная команда отключает логирование фильтрации DHCP-сообщений при помощи приложения DHCP Snooping.

Формат no ip dhcp snooping log-invalid

Режим Interface Config

ip dhcp snooping trust

Данная команда настраивает интерфейс или диапазон интерфейсов в качестве доверенного.

По умолчанию отключено

Формат ip dhcp snooping trust

Режим Interface Config

no ip dhcp snooping trust

Данная команда настраивает порт как недоверенный.

Формат no ip dhcp snooping trust

Режим Interface Config

show ip dhcp snooping

Данная команда отображает настройки DHCP Snooping: глобальные и для конкретных портов.

Формат show ip dhcp snooping

Режим Privileged EXEC

Термин	Значение
Interface	Интерфейс, для которого отображаются данные.
Trusted	Если этот параметр включен, DHCP snooping считает этот порт доверенным. По умолчанию - выключен.
Log Invalid Pkts	Если этот параметр включен, приложение DHCP snooping журналирует некорректные пакеты на указанном интерфейсе.

ПРИМЕР: Вывод командной строки для данной команды.

```
(switch) #show ip dhcp snooping
DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
11 - 30, 40
```

Interface	Trusted	Log Invalid Pkts
0/1	Yes	No
0/2	No	Yes
0/3	No	Yes
0/4	No	No
0/6	No	No

show ip dhcp snooping binding

Данная команда отображает записи привязки DHCP Snooping. Для ограничения вывода команды используйте следующие параметры:

- Dynamic: Ограничить вывод на основе DCHP snooping.
- Interface: Ограничить вывод на основе указанного интерфейса.
- Static: Ограничить вывод на основе статических записей.

Формат show ip dhcp snooping binding [{static/dynamic}] [interface unit/slot/port] [vlan id]

Режим Privileged EXEC

Термин	Значение
MAC Address	Отображает MAC-адрес, добавленный для привязки. MAC-адрес - это ключевой параметр базы данных привязки.
IP Address	Отображает действительный IP-адрес для правила привязки.
VLAN	VLAN для правила привязки.
Interface	Интерфейс для добавления привязки к интерфейсу DHCP snooping.
Type	Тип привязки: динамическая или статически настроенная при помощи командной строки.
Lease (sec)	Оставшееся время аренды для записи.

ПРИМЕР: Вывод командной строки для данной команды.

```
(switch) #show ip dhcp snooping binding
Total number of bindings: 2
```

MAC Address	IP Address	VLAN	Interface	Type	Lease time (Secs)
00:02:B3:06:60:80	210.1.1.3	10	0/1		86400
00:0F:FE:00:13:04	210.1.1.4	10	0/1		86400

show ip dhcp snooping database

Данная команда отображает конфигурацию DHCP Snooping, имеющую отношение к месту хранения базы данных.

Формат show ip dhcp snooping database

Режим Privileged EXEC

Термин	Значение
Agent URL	URL агента базы данных.
Write Delay	Максимальное время записи базы данных на локальное или удаленное хранилище.

ПРИМЕР: Вывод командной строки для данной команды.

```
(switch) #show ip dhcp snooping database agent url:/10.131.13.79:/sai1.txt
write-delay:  5000
```

show ip dhcp snooping interfaces

Данная команда отображает состояние DHCP Snooping на интерфейсах.

Формат show ip dhcp snooping interfaces

Режим Privileged EXEC

ПРИМЕР: Пример вывода командной строки для данной команды.

```
(switch) #show ip dhcp snooping interfaces
```

Interface	Trust State	Rate Limit (pps)	Burst Interval (seconds)
1/g1	No	15	1
1/g2	No	15	1
1/g3	No	15	1

```
(switch) #show ip dhcp snooping interfaces ethernet 1/g15
```

Interface	Trust State	Rate Limit(pps)	Burst Interval (seconds)
1/g15	Yes	15	1

show ip dhcp snooping statistics

Данная команда отображает статистику нарушений безопасности DHCP Snooping на недоверенных портах.

Формат show ip dhcp snooping statistics

Режим Privileged EXEC

Термин	Значение
Interface	IP-адрес интерфейса в формате unit/slot/port.
Термин	Значение
MAC Verify Failures	Количество сообщений DHCP, которые были отфильтрованы на недоверенных интерфейсах по причине несовпадения MAC-адреса источника и аппаратного адреса клиента.
Client Ifc Mismatch	Количество сообщений DHCP release и Deny, полученных не на тех портах, которые были изучены ранее.
DHCP Server Msgs Rec'd	Количество сообщений сервера DHCP, полученных на недоверенных портах.

ПРИМЕР: Вывод командной строки для данной команды.

(switch) #show ip dhcp snooping statistics

Interface	MAC Verify Failures	Client Ifc Mismatch	DHCP Server Msgs Rec'd
1/0/2	0	0	0
1/0/3	0	0	0
1/0/4	0	0	0
1/0/5	0	0	0
1/0/6	0	0	0
1/0/7	0	0	0
1/0/8	0	0	0

clear ip dhcp snooping binding

Данная команда удаляет все привязки DHCP Snooping на всех интерфейсах (либо на указанном интерфейсе).

Формат clear ip dhcp snooping binding [interface *unit/slot/port*]

Режим Privileged EXEC

clear ip dhcp snooping statistics

Данная команда очищает всю статистику DHCP Snooping.

Формат clear ip dhcp snooping statistics

Режим Privileged EXEC

7.20. Команды конфигурации IGMP Snooping

В этом разделе описаны команды, которые используются для настройки IGMP snooping. ПО коммутатора поддерживает IGMP версий 1, 2 и 3. Функция IGMP Snooping помогает распределять полосу пропускания более экономно, перенаправляя многоадресный IP-трафик только на те подключенные хосты, которые запрашивают многоадресный трафик. IGMPv3 добавляет возможность фильтрации по источнику, к IGMP версий 1 и 2.

ПРИМЕЧАНИЕ: Многие команды IGMP/MLD Snooping доступны как в режиме Interface, так и в режиме VLAN. Во время работы система предпочитает настроенные значения VLAN перед настроенным параметрам интерфейса для большинства конфигураций, когда интерфейс участвует в VLAN

set igmp

Данная команда включает IGMP Snooping глобально (в режиме Global Config) либо на интерфейсе или диапазоне интерфейсов. Данная команда также включает IGMP Snooping на указанной VLAN (в режиме VLAN Config) и на всех интерфейсах, принадлежащих VLAN.

Функциональность IGMP Snooping на интерфейсе отключается, если интерфейс включается для маршрутизации либо указывается как член агрегированного канала (LAG). После устранения этих условий, то есть после отключения маршрутизации либо удаления членства в агрегированном канале, IGMP Snooping начинает работать снова (если до этого функция была включена).

Приложение IGMP поддерживает следующее:

- Проверка контрольной суммы заголовка IP (а также контрольной суммы заголовка IGMP) и отбрасывание фрейма при ошибке контрольной суммы.
- Ведение записей таблицы переадресации на основе MAC- и IP-адресов.
- Распространения незарегистрированных пакетов мультикаст данных на все порты VLAN.

По умолчанию отключено

Формат set igmp [*vlan_id*]

Режим Global Config
Interface Config
VLAN Config

no set igmp

Данная команда отключает IGMP Snooping в системе, на интерфейсе, диапазоне интерфейсов или в сети VLAN.

Формат no set igmp [*vlan_id*]

Режим Global Config

Interface Config

VLAN Config

set igmp header-validation

Данная команда включает функцию проверки заголовка сообщений IGMP.

Если функция включена, проверяются следующие параметры:

- Поле TTL в заголовке IGMP (и отбрасывает пакеты, где TTL не равен 1). Поле TTL в заголовках IGMP report и query всегда должно быть установлено на 1 .
- Наличие опции router alert в заголовке IP-пакета сообщения IGMPv2 (и отбрасывает пакеты, которые не включают эту опцию).
- Наличие опции router alert и ToS Byte = 0xC0 (Internet Control) в заголовке IP-пакета сообщения IGMPv3 (и отбрасывает пакеты, которые не включают эти параметры).

По умолчанию включено

Формат set igmp header-validation

Режим Global Config

no set igmp header-validation

Данная команда отключает функцию проверки заголовка сообщений IGMP.

Формат no set igmp header-validation

Режим Global Config

set igmp interfacemode

Данная команда включает IGMP Snooping на всех интерфейсах. Функциональность IGMP Snooping на интерфейсе отключается, если интерфейс включается для маршрутизации либо зачисляется как член агрегированного канала (LAG). После отключения маршрутизации либо удаления членства в агрегированном канале, IGMP Snooping начинает работать снова (если до этого функция была включена).

По умолчанию отключено

Формат set igmp interfacemode

Режим Global Config

no set igmp interfacemode

Данная команда отключает IGMP Snooping на всех интерфейсах.

Формат no set igmp interfacemode

Режим Global Config

set igmp fast-leave

Данная команда включает режим IGMP Snooping fast-leave, на интерфейсе, диапазоне интерфейсов или в сети VLAN. Включение fast-leave позволяет коммутатору немедленно удалить интерфейс L2 таблицы переадресации мультикаста при получении сообщения о IGMP leave для этой многоадресной группы без предварительной отправки general query на основе MAC на интерфейс.

Включать режим fast-leave следует только в тех VLAN, в которых к каждому порту L2 LAN подключен только один хост. Это предотвращает непреднамеренное отключение других хостов, которые были подключены к одному порту L2 LAN, но все еще заинтересованы в получении многоадресного трафика, направленного на эту группу. Кроме того, обработка fast-leave поддерживается только с хостами IGMP версии 2.

По умолчанию отключено

Формат set igmp fast-leave [*vlan_id*]

Режим Interface Config

Interface Range

VLAN Config

no set igmp fast-leave

Данная команда отключает режим IGMP Snooping fast-leave на выбранном интерфейсе.

Формат no set igmp fast-leave [*vlan_id*]

Режим Interface Config

Interface Range

VLAN Config

set igmp groupmembership-interval

Эта команда устанавливает время IGMP Group Membership Interval на интерфейсе, диапазоне интерфейсов, на всех интерфейсах либо в сети VLAN. The Group Membership Interval - это время (в секундах), в течение которого коммутатор ожидает report от конкретной группы на конкретном интерфейсе перед удалением интерфейса из записи таблицы. Это значение должно быть больше, чем значение максимальное время отклика IGMPv3. Диапазон - от 2 до 3600 секунд.

По умолчанию 260 секунд

Формат set igmp groupmembership-interval [*vlan_id*] *2-3600*

Режим nterface Config

Global Config

VLAN Config

no set igmp groupmembership-interval

Данная команда сбрасывает значение IGMPv3 Group Membership Interval на настройки по умолчанию.

Формат no set igmp groupmembership-interval [*vlan_id*]

Режим Interface Config

Global Config

VLAN Config

set igmp maxresponse

Данная команда устанавливает максимальное время отклика IGMP системы, на интерфейсе, диапазоне интерфейсов или в сети VLAN. Maximum Response time - это время ожидания коммутатора после отправки query на интерфейс (в секундах), в том случае, если он не получит report для определенной группы в этом интерфейсе. Это значение должно быть больше, чем значение IGMP Query Interval. Диапазон - от 1 до 25 секунд.

По умолчанию 10 секунд

Формат set igmp maxresponse [*vlan_id*] *1-25*

Режим Global Config

Interface Config

VLAN Config

no set igmp maxresponse

Данная команда сбрасывает значение max response time (на интерфейсе или VLAN) настройки по умолчанию.

Формат no set igmp maxresponse [*vlan_id*]

Режим Global Config

Interface Config

VLAN Config

set igmp mcrtrexpiretime

Данная команда устанавливает значение Multicast Router Present Expiration time. Команда устанавливает временное значение для системы, на интерфейсе, диапазоне интерфейсов или сети VLAN. Значение Multicast Router Present Expiration time представляет собой количество времени (в секундах), в течение которого коммутатор ожидает получения query на интерфейсе до того, как интерфейс будет удален из списка интерфейсов с подключенными многоадресными маршрутизаторами. Диапазон - от 0 до 3600 секунд. Нулевое значение – бесконечный таймаут, то есть без истечения срока.

По умолчанию 0

Формат set igmp mcrtrexpiretime [*vlan_id*] *0-3600*

Режим Global Config

Interface Config

VLAN Config

no set igmp mcrtrexpiretime

Данная команда устанавливает значение Multicast Router Present Expiration time на 0. Команда устанавливает временное значение для конкретного интерфейса или VLAN.

Формат no set igmp mcrtrexpiretime [*vlan_id*]

Режим Global Config

Interface Config

VLAN Config

set igmp mrouter

Данная команда настраивает VLAN ID (*vlan_id*) в котором находится многоадресный маршрутизатор.

Формат set igmp mrouter vlan_id

Режим Interface Config

no set igmp mrouter

Данная команда отключает режим многоадресного маршрутизатора для определенного VLAN ID (*vlan_id*).

Формат no set igmp mrouter *vlan_id*

Режим Interface Config

set igmp mrouter interface

Данная команда настраивает интерфейс либо диапазон интерфейсов в качестве интерфейса многоадресного маршрутизатора. После настройки такой интерфейс обрабатывается как интерфейс многоадресного маршрутизатора во всех VLAN.

По умолчанию отключено

Формат set igmp mrouter interface

Режим Interface Config

no set igmp mrouter interface

Данная команда отключает на интерфейсе режим статически настроенного многоадресного маршрутизатора.

Формат no set igmp mrouter interface

Режим Interface Config

set igmp report-suppression

Используйте эту команду для подавления IGMP report по указанному VLAN ID. Данная функция используется для оптимизации количества report, проходящих через сеть без необходимости. Когда на IGMP query для одного и того же адреса группы в пределах max-responsetime реагируют несколько клиентов, только первый report перенаправляется на query, а остальные подавляются на коммутаторе.

По умолчанию Disabled (Отключено)

Формат set igmp report-suppression vlan-id

Режим VLAN Config

Global config

Параметр	Описание
vlan-id	Действительный идентификатор VLAN. Диапазон - от 1 до 4094.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Switching) #vlan database
(Switching) (Vlan)#set igmp report-suppression ?
<1-4093>        Enter VLAN ID.
(Switching) (Vlan)#set igmp report-suppression 1
```

no set igmp report-suppression

Данная команда возвращает системе настройки по умолчанию.

Формат no set igmp report-suppression

Режим VLAN Config

Global Config

show igmpsnooping

Данная команда отображает информацию, касающуюся IGMP Snooping, для определенного *unit/slot/port* либо VLAN. Конфигурация настроек отображается независимо от того, включен ли IGMP Snooping на данный момент или нет.

Формат show igmpsnooping [*unit/slot/port* | *vlan_id*]

Режим Privileged EXEC

Если не указаны необязательные параметры *unit/slot/port* либо *vlan_id*, отображается следующая информация:

Термин	Значение
Admin Mode	Включена ли функция IGMP Snooping на коммутаторе.
Multicast Control Frame Count	Количество управляющих многоадресных фреймов, обработанных ЦП.
Interface Enabled for IGMP Snooping	Список интерфейсов, на которых включена функция IGMP Snooping.

Термин	Значение
VLANS Enabled for IGMP Snooping	Список VLAN, на которых включена функция IGMP Snooping.

Если необязательные параметры *unit/slot/port* либо *vlan_id* указаны, отображается следующая информация:

Термин	Значение
IGMP Snooping Admin Mode	Включена ли функция IGMP Snooping на интерфейсе.
Fast Leave Mode	Включена ли функция IGMP Snooping Fast-leave на интерфейсе.
Group Membership Interval	Время (в секундах), в течение которого коммутатор ожидает report от конкретной группы на конкретном интерфейсе перед удалением этого интерфейса из записи. Это значение может быть настроено.
Maximum Response Time	Время ожидания коммутатора после отправки query на интерфейс (в секундах), в том случае если он не получит report для определенной группы в этом интерфейсе. Это значение может быть настроено.
Multicast Router Expiry Time	Время ожидания перед тем как коммутатор удаляет интерфейс из списка интерфейсов с подключенными многоадресными маршрутизаторами. Интерфейс удаляется в том случае, если query не получен. Это значение может быть настроено.

Если указано значение `vlan_id`, отображается следующая информация:

Термин	Значение
VLAN ID	Идентификатор VLAN.
IGMP Snooping Admin Mode	Включена ли функция IGMP Snooping на указанной VLAN.
Fast Leave Mode	Включена ли функция IGMP Snooping Fast-leave на указанной VLAN.
Group Membership Interval (secs)	Время (в секундах), в течение которого коммутатор ожидает report от конкретной группы на конкретном интерфейсе перед удалением этого интерфейса из записи. Это значение может быть настроено.

Термин	Значение
Maximum Response Time (secs)	Время ожидания коммутатора после отправки query на интерфейс, принимающий участие в VLAN, в том случае, если он не получит report для определенной группы в этом интерфейсе. Это значение может быть настроено.
Multicast Router Expiry Time (secs)	Время, в течение которого коммутатор ожидает получения query на интерфейсе до того, как интерфейс будет удален из списка интерфейсов с подключенными многоадресными маршрутизаторами. Интерфейс удаляется в том случае, если query не получен. Это значение может быть настроено.
Report Suppression Mode	Включено ли подваление report.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Switching) #show igmpsnooping 1
VLAN ID ..... 1
IGMP Snooping Admin Mode ..... Disabled
Fast Leave Mode ..... Disabled
Group Membership Interval (secs) ..... 260
Max Response Time (secs) ..... 10
Multicast Router Expiry Time (secs) ..... 0
Report Suppression Mode ..... Enabled
```

show igmpsnooping mrouter interface

Данная команда отображает информацию о статически настроенных портах.

Формат show igmpsnooping mrouter interface *unit/slot/port*

Режим Privileged EXEC

Термин	Значение
Interface	Порт, о котором отображается информация многоадресной маршрутизации.
Multicast Router Attached	Включен ли статически многоадресный маршрутизатор на интерфейсе или нет
VLAN ID	Список VLAN, членом которых является данный интерфейс.

show igmpsnooping mrouter vlan

Данная команда отображает информацию о статически настроенных портах.

Формат show igmpsnooping mrouter vlan *unit/slot/port*

Режим Privileged EXEC

Термин	Значение
Interface	Порт, о котором отображается информация многоадресной маршрутизации.
VLAN ID	Список VLAN, членом которых является данный интерфейс.

show mac-address-table igmpsnooping

Эта команда отображает записи IGMP Snooping в таблице MFDB.

Формат show mac-address-table igmpsnooping

Режим Privileged EXEC

Термин	Значение
VLAN ID	VLAN, в которой изучен MAC-адрес.
MAC Address	Многоадресный MAC-адрес, для которого коммутатор имеет информацию о перенаправлении или фильтрации. Формат - 6 двухзначных шестнадцатеричных чисел, разделенных двоеточиями, например 01:23:45:67:89:AB.
Type	Тип записи, которая может быть либо статической (добавленной пользователем), либо динамической (добавляется в таблицу втоматически).
Описание	Текстовое описание записи.
Interfaces	Список интерфейсов, предназначенных для перенаправления (Fwd:) и фильтрации (Flt:).

7.21. Команды конфигурации IGMP Snooping Querier

IGMP Snooping требует, чтобы один центральный коммутатор или маршрутизатор периодически запрашивал от всех конечных устройства в сети, объявлений их многоадресного членства. Это центральное устройство и называется генератором запросов (IGMP Querier). Ответы на IGMP-Query, также известные как IGMP-Report, поддерживают обновление коммутатора в соответствии с текущим членством в группе многоадресной рассылки по принципу порт за портом. Если коммутатор не получает обновленную информацию о членстве своевременно, он прекращат переадресацию многоадресной рассылки на порт, где находится конечное устройство.

В этом разделе описываются команды, используемые для настройки и отображения информации IGMP Snooping Querier в сети и, отдельно, в сетях VLAN.

ПРИМЕЧАНИЕ: Многие команды IGMP/MLD Snooping доступны как в режиме Interface, так и в режиме VLAN. Во время работы система предпочитает настроенные значения VLAN перед настроенным параметрам интерфейса для большинства конфигураций, когда интерфейс участвует в VLAN.

set igmp querier

Данная команда используется для включения IGMP Snooping Querier во всей системе (режим Global Config) либо на VLAN. С помощью этой команды можно указать IP-адрес для использования IGMP Snooping Querier при, собственно, отправке периодических query.

Если в сети VLAN включен IGMP Snooping Querier, но при этом отключен IGMP Snooping, функция IGMP Snooping Querier также будет отключена в данной VLAN. После повторного включения IGMP Snooping функция Querier также включается.

ПРИМЕЧАНИЕ: IP-адрес, назначенный для VLAN, имеет приоритет перед глобальной конфигурацией.

Приложение IGMP Snooping Querier поддерживает отправку периодических General Query во VLAN для запроса Report о членстве.

По умолчанию отключено

Формат set igmp querier [*vlan-id*] [address *ipv4_address*]

Режим Global Config

VLAN Mode

no set igmp querier

Данная команда отключает IGMP Snooping Querier в системе. Необязательный параметр address также сбрасывает адрес Querier на 0.0.0.0.

Формат no set igmp querier [*vlan-id*] [address]

Режим Global Config

VLAN Mode

set igmp querier query-interval

Данная команда позволяет настроить время интервала запросов IGMP Snooping Querier. Другими словами, это промежуток времени (в секундах), на протяжении которого коммутатор ожидает перед отправкой другого General Query.

По умолчанию отключено

Формат set igmp querier query-interval *1-1800*

Режим Global Config

no set igmp querier query-interval

Данная команда сбрасывает время интервала запросов IGMP Snooping Querier на настройки по умолчанию.

Формат no set igmp querier query-interval

Режим Global Config

set igmp querier timer expiry

Данная команда позволяет настроить период истечения таймера IGMP Snooping Querier. Это период времени, в течение которого коммутатор остается в режиме Non-Querier после обнаружения в сети другого Querier.

По умолчанию 60 секунд

Формат set igmp querier timer expiry 60-300

Режим Global Config

no set igmp querier timer expiry

Данная команда сбрасывает период истечения время таймера IGMP Snooping Querier на настройки по умолчанию.

Формат no set igmp querier timer expiry

Режим Global Config

set igmp querier version

Данная команда используется для настройки версии IGMP для Query, которые коммутатор будет периодически рассылать.

По умолчанию 1

Формат set igmp querier version *1-2*

Режим Global Config

no set igmp querier version

Данная команда сбрасывает версию рассылаемы IGMP Query на настройки по умолчанию.

Формат no set igmp querier version

Режим Global Config

set igmp querier election participate

Данная команда активирует участие Querier в процессе выбора при обнаружении в сети VLAN другого Querier. Когда этот режим включен, то Querier прекращает рассылку своих периодических запросов при обнаружении другого Querier с «меньшим» адресом источника. Если в результате процесса выбора приоритет получит именно этот Querier, то он продолжит свою работу.

По умолчанию отключено

Формат set igmp querier election participate

Режим VLAN Config

no set igmp querier election participate

Данная команда отменяет участие Querier в процессе выбора. Обратите внимание, что в этом случае при обнаружении в сети VLAN другого Querier данный Querier прекращает работу.

Формат no set igmp querier election participate

Режим VLAN Config

show igmpsnooping querier

Данная команда отображает информацию о IGMP Snooping Querier. Конфигурация настроек отображается независимо от того, включен ли Querier на данный момент или нет.

Формат show igmpsnooping querier [{detail | vlan *vlanid*}]

Режим Privileged EXEC

Если не указан необязательный параметр **vlanid**, отображается следующая информация.

Поле	Описание
Admin Mode	Включена ли функция IGMP Snooping Querier на коммутаторе.
Admin Version	Версия IGMP, используемая при рассылке Query.
Querier Address	IP-адрес, используемый в заголовке IPv4 при отправке IGMP-Query. Может быть настроен при помощи соответствующей команды.
Query Interval	Промежуток времени ожидания перед отправкой периодического General Query (в секундах).
Querier Timeout	Промежуток времени ожидания в состоянии Non-Querier перед переключением в состояние Querier.

При указании **vlanid** будет отображаться следующая дополнительная информация.

Поле	Описание
VLAN Admin Mode	Включена ли функция IGMP Snooping Querier на данной VLAN.
VLAN Operational State	Находится ли коммутатор в состоянии “Querier” либо “Non-Querier”. Если коммутатор находится в состоянии *Querier* – он рассылает периодические General Query. Если коммутатор находится в состоянии *Non-Querier* – то Query не рассылаются до тех пор, пока устройство снова не перейдет в режим «Querier».
VLAN Operational Max Response Time	Время ожидания перед удалением «Leave» с хоста после получения запроса «Leave». Это значение динамически рассчитывается из Queries, полученных в сети. Если коммутатор находится в состоянии Querier, то оно равно настроенному значению.

Поле	Описание
Querier Election Participation	Участвует ли данный Querier в процессе выбора, в том случае если он обнаруживает присутствие во VLAN еще одного Querier
Querier VLAN Address	IP-адрес, используемый в заголовке IPv4 при отправке IGMP-query. Может быть настроен при помощи соответствующей команды.
Operational Version	Версия IPv4, используемая при рассылке IGMP Query в данной VLAN.
Last Querier Address	IP-адрес Querier, от которого был получен последний Query.
Last Querier Version	Версия IGMP последнего Querier, отправившего Query в данной VLAN.

При использовании необязательного аргумента detail команда отображает глобальную информацию, а также информацию обо всех VLAN со включенным Querier.

7.22. Команды MLD Snooping

В этом разделе описываются команды, используемые для MLD Snooping. В IPv4 коммутаторы уровня 2 OSI могут использовать IGMP Snooping для ограничения многоадресного трафика путем динамической настройки интерфейсов уровня 2, так что многоадресный трафик перенаправляется только на те интерфейсы, которые ассоциированы с многоадресными IP-адресами. MLD Snooping выполняет схожие функции в IPv6. С MLD Snooping многоадресные данные IPv6 выборочно пересылаются только на список портов, которые хотят получать данные, вместо того, чтобы рассылаться на все порты во VLAN. Этот список портов формируется перехватом управляющих мультикастом пакетов IPv6.

ПРИМЕЧАНИЕ: Многие команды IGMP/MLD Snooping доступны как в режиме Interface, так и в режиме VLAN. Во время работы система предпочитает настроенные значения VLAN перед настроенным параметрам интерфейса для большинства конфигураций, когда интерфейс участвует в VLAN.

set mld

Данная команда включает MLD Snooping глобально (в режиме Global Config) либо на интерфейсе или диапазоне интерфейсов. Данная команда также включает MLD Snooping на указанной VLAN и всех интерфейсах, принадлежащих VLAN.

Функциональность MLD Snooping на интерфейсе отключается, если интерфейс включенается для маршрутизации либо зачисляется как член агрегированного канала (LAG). После устранения этих условий, то есть после отключения маршрутизации либо удаления членства в агрегированном канале, MLD Snooping начинает работать снова (если до этого функция была включена).

Приложение MLD Snooping поддерживает следующее:

- Проверка версии адреса, согласованности длины полезных данных и отбрасывание фреймов в случае ошибки.
- Ведение записей таблицы переадресации на основе MAC- и IPv6-адресов.
- Распространения незарегистрированных пакетов данных на все порты VLAN.

По умолчанию отключено

Формат set mld *vlanid*

Mode Global Config
Interface Config
VLAN Mode

no set mld

Данная команда отключает MLD Snooping в системе

Формат set mld *vlanid*

Режим Global Config
Interface Config
VLAN Mode

set mld interfacemode

Данная команда включает MLD Snooping на всех интерфейсах. Функциональность MLD Snooping на интерфейсе отключается, если интерфейс включенается для маршрутизации либо зачисляется как член агрегированного канала (LAG). После устранения этих условий, то есть после отключения маршрутизации либо удаления членства в агрегированном канале, MLD Snooping начинает работать снова (если до этого функция была включена)

По умолчанию отключено

Формат set mld interfacemode

Режим Global Config

no set mld interfacemode

Данная команда отключает MLD Snooping на всех интерфейсах.

Формат no set mld interfacemode

Режим Global Config

set mld fast-leave

Данная команда включает режим MLD Snooping fast-leave на выбранном интерфейсе или VLAN. Включение fast-leave позволяет коммутатору немедленно удалить интерфейс LAN 2 уровня из таблицы переадресации при получении сообщения MLD done для этой многоадресной группы без предварительной отправки general query на основе MAC на интерфейс.

ПРИМЕЧАНИЕ: Включать режим fast-leave следует только в тех VLAN, в которых к каждому порту LAN уровня 2 подключен только один хост. Это предотвращает

непреднамеренное отключение других хостов, которые были подключены к одному порту LAN уровня 2, но все еще заинтересованы в получении многоадресного трафика, направленного на эту группу.

ПРИМЕЧАНИЕ: Кроме того, обработка fast-leave поддерживается только с хостами MLD версии 1.

По умолчанию отключено

Формат set mld fast-leave *vlan_id*

Режим Interface Config

VLAN Mode

no set mld fast-leave

Данная команда отключает режим MLD Snooping fast-leave на выбранном интерфейсе.

Формат no set mld fast-leave *vlan_id*

Режим Interface Config

VLAN Mode

set mld groupmembership-interval

Эта команда устанавливает время MLD Group Membership Interval на интерфейсе, на всех интерфейсах либо в сети VLAN. The Group Membership Interval - это время (в секундах), в течение которого коммутатор ожидает report от конкретной группы на конкретном интерфейсе перед удалением интерфейса из записи. Это значение должно быть больше, чем значение максимального времени отклика MLDv2. Диапазон - от 2 до 3600 секунд.

По умолчанию 260 секунд

Формат set mld groupmembership-interval *vlanid 2-3600*

Режим Interface Config

Global Config

VLAN Mode

no set groupmembership-interval

Данная команда сбрасывает значение MLDv2 Group Membership Interval на настройки по умолчанию.

Формат no set mld groupmembership-interval

Режим Interface Config

Global Config

VLAN Mode

set mld maxresponse

Данная команда устанавливает максимальное время отклика MLD в системе, на интерфейсе или на определенном интерфейсе VLAN. Maximum Response time - это время ожидания коммутатора после отправки query на интерфейс (в секундах), в том случае,

если он не получит report для определенной группы в этом интерфейсе. Это значение должно быть больше, чем значение MLD Query Interval. Диапазон - от 1 до 65 секунд.

По умолчанию 10 секунд

Формат set mld maxresponse 1-65

Режим Global Config

Interface Config

VLAN Mode

no set mld maxresponse

Данная команда сбрасывает значение max response time (на интерфейсе или VLAN) настройки по умолчанию.

Формат no set mld maxresponse

Режим Global Config

Interface Config

VLAN Mode

set mld maxresponse

Данная команда устанавливает значение Multicast Router Present Expiration time. Команда устанавливает временное значение для конкретного интерфейса или VLAN. Значение Multicast Router Present Expiration time представляет собой количество времени (в секундах), в течение которого коммутатор ожидает получения query на интерфейсе до того, как интерфейс будет удален из списка интерфейсов с подключенными многоадресными маршрутизаторами. Диапазон - от 0 до 3600 секунд. Нулевое значение – бесконечный таймаут, то есть без истечения срока.

По умолчанию 0

Формат set mld mcrtexpiretime *vlanid 0-3600*

Режим Global Config

Interface Config

no set mld mcrtexpiretime

Данная команда устанавливает значение Multicast Router Present Expiration time 0. Команда устанавливает временное значение для конкретного интерфейса или VLAN.

Формат no set mld mcrtexpiretime *vlanid*

Режим Global Config

Interface Config

set mld mrouter

Данная команда настраивает VLAN ID для VLAN со включенным режимом Multicast Router attached.

Формат set mld mrouter *vlanid*

Режим Interface Config

no set mld mrouter

Данная команда отключает режим Multicast Router attached для VLAN с указанным VLAN ID.

Формат no set mld mrouter *vlanid*

Режим Interface Config

set mld mrouter interface

Данная команда настраивает интерфейс в качестве интерфейса, подключенного к маршрутизатору. После настройки такой интерфейс обрабатывается как многоадресный интерфейс, подключенный к маршрутизатору, во всех VLAN.

По умолчанию отключено

Формат set mld mrouter interface

Режим Interface Config

no set mld mrouter interface

Данная команда отключает на интерфейсе режим статически настроенного многоадресного маршрутизатора.

Формат no set mld mrouter interface

Режим Interface Config

show mldsnooping

Данная команда отображает информацию, относящуюся к MLD Snooping. Конфигурация настроек отображается независимо от того, включен ли MLD Snooping на данный момент или нет.

Формат show mldsnooping [unit/slot/port | vlanid]

Режим Privileged EXEC

Если не указаны необязательные параметры **unit/slot/port** либо **vlanid**, отображается следующая информация.

Термин	Значение
Admin Mode	Включена ли функция MLD Snooping на коммутаторе.
Interfaces Enabled for MLD Snooping	Интерфейсы, на которых включена функция MLD snooping.
MLD Control Frame Count	Количество управляющих многоадресных фреймов MLD, обработанных ЦП.
VLANs Enabled for MLD Snooping	VLANы, на которых влючена функция MLD Snooping

При указании значений **unit/slot/port** отображается следующая информация.

Термин	Значение
Snooping Admin Mode	Включена ли функция MLD Snooping на интерфейсе.
Fast Leave Mode	Включена ли функция MLD Snooping Fast Leave на указанной VLAN.
Group Membership Interval	Время (в секундах), в течение которого коммутатор ожидает report от конкретной группы на конкретном интерфейсе, участвующем во VLAN, перед удалением этого интерфейса из записи. Это значение может быть настроено
Maximum Response Time	Время ожидания коммутатора после отправки query на интерфейс, принимающий участие в VLAN, в том случае, если он не получит report для определенной группы в этом интерфейсе. Это значение может быть настроено.
Multicast Router Present Expiration Time	Время, в течение которого коммутатор ожидает получения query на интерфейсе до того, как интерфейс будет удален из списка интерфейсов с подключенными многоадресными маршрутизаторами. Интерфейс удаляется в том случае, если query не получен. Это значение может быть настроено.

Если указано значение **vlanid**, отображается следующая информация.

Термин	Значение
VLAN Admin Mode	Включена ли функция MLD Snooping на данной VLAN.

show mldsnooping mrouter interface

Данная команда отображает информацию о статически настроенных интерфейсах, подключенных к многоадресному маршрутизатору.

Формат show mldsnooping mrouter interface *unit/slot/port*

Режим Privileged EXEC

Термин	Значение
Interface	Интерфейс, о котором отображается информация многоадресной маршрутизации.
Multicast Router Attached	Включен ли статически многоадресный маршрутизатор на интерфейсе или нет.

Термин	Значение
VLAN ID	Список VLAN, членом которых является данный интерфейс.

show mldsnooping mrouter vlan

Данная команда отображает информацию о статически настроенных интерфейсах, подключенных к многоадресному маршрутизатору.

Формат show mldsnooping mrouter vlan *unit/slot/port*

Режим Privileged EXEC

Термин	Значение
Interface	Интерфейс, о котором отображается информация многоадресной маршрутизации.
VLAN ID	Список VLAN, членом которых является данный интерфейс.

show mac-address-table mldsnooping

Данная команда отображает записи MLD Snooping в таблице MFDB (Multicast Forwarding Database).

Формат show mac-address-table mldsnooping

Режим Privileged EXEC

Термин	Значение
VLAN ID	VLAN, в которой изучен MAC-адрес.
MAC Address	Многоадресный MAC-адрес, для которого коммутатор имеет информацию о перенаправлении или фильтрации. Формат - 6 двухзначных шестнадцатеричных чисел, разделенных двоеточиями, например 01:23:45:67:89:AB.
Type	Тип записи, которая может быть либо статической (добавленной пользователем), либо динамической (добавляется в таблицу автоматически).
Описание	Текстовое описание записи.
Interfaces	Список интерфейсов, предназначенных для перенаправления (Fwd:) и фильтрации (Flt:).

clear mldsnooping

Данная команда удаляет все записи MLD Snooping из таблицы MFDB.

Формат clear mldsnooping

Режим Privileged EXEC

7.23. Команды конфигурации MLD Snooping Querier

В сетях IPv6, MLD Snooping требует, чтобы один центральный коммутатор или маршрутизатор периодически запрашивал все конечные устройства в сети, чтобы они объявили свои многоадресные членства. Это центральное устройство и называется генератором запросов MLD (MLD Querier). Ответы на MLD-Query, также известные как MLD-Report, поддерживают обновление коммутатора в соответствии с текущим членством в группе многоадресной рассылки по принципу порт за портом. Если коммутатор не получает обновленную информацию о членстве своевременно, он прекращат переадресацию многоадресной рассылки на порт, где находится конечное устройство.

В этом разделе описываются команды, используемые для настройки и отображения информации MLD Snooping Querier в сети и, отдельно, в сетях VLAN.

ПРИМЕЧАНИЕ: Многие команды IGMP/MLD Snooping доступны как в режиме Interface, так и в режиме VLAN. Во время работы система предпочитает настроенные значения VLAN перед настроенным параметрам интерфейса для большинства конфигураций, когда интерфейс участвует в VLAN.

set mld querier

Данная команда используется для включения MLD Snooping Querier во всей системе (режим Global Config) либо во VLAN. С помощью этой команды можно указать IP-адрес для использования MLD Snooping Querier при, собственно, отправке периодических Query.

Если в сети VLAN включен MLD Snooping Querier, но при этом отключен MLD Snooping, функция Querier также будет отключена в данной VLAN. После повторного включения MLD Snooping функция Querier также включается.

Приложение MLD Snooping Querier поддерживает отправку периодических General Query во VLAN для запроса Report о членстве.

По умолчанию отключено

Формат set mld querier [*vlan-id*] [address *ipv6_address*]

Режим Global Config

VLAN Mode

no set mld querier

Данная команда отключает MLD Snooping Querier в системе Необязательный параметр address также сбрасывает адрес Querier на 0.0.0.0.

Формат no set mld querier [*vlan-id*][address]

Режим Global Config

VLAN Mode

set mld querier query-interval

Данная команда позволяет настроить время интервала запросов MLD Snooping Querier. Другими словами, это промежуток времени (в секундах), на протяжении которого коммутатор ожидает перед отправкой другого general query.

По умолчанию	60 секунд
Формат	set mld querier query-interval *1-1800*
Режим	Global Config

no set mld querier query-interval

Данная команда сбрасывает время интервала запросов MLD Snooping Querier на настройки по умолчанию.

Формат	no set mld querier query-interval
Режим	Global Config

set mld querier timer expiry

Данная команда позволяет настроить период истечения время таймера MLD Snooping Querier. Это период времени, в течение которого коммутатор остается в режиме Non-Querier после обнаружения в сети другого Querier.

По умолчанию	60 секунд
Формат	set mld querier timer expiry *60-300*
Режим	Global Config

no set mld querier timer expiry

Данная команда сбрасывает период истечения таймера MLD Snooping Querier на настройки по умолчанию.

Формат	no set mld querier timer expiry
Режим	Global Config

set mld querier election participate

Данная команда активирует участие Querier в процессе выбора при обнаружении в сети VLAN другого Querier. Когда этот режим включен, то Querier прекращает рассылку своих периодических запросов при обнаружении другого Querier с «меньшим» адресом источника. Если в результате процесса выбора приоритет получит именно этот Querier, то он продолжит свою работу.

По умолчанию	отключено
Формат	set mld querier election participate
Режим	VLAN Config

no set mld querier election participate

Данная команда отменяет участие Querier в процессе выбора. Обратите внимание, что в этом случае при обнаружении в сети VLAN другого Querier данный Querier прекращает работу.

Формат no set mld querier election participate

Режим VLAN Config

show mldsnooping querier

Данная команда отображает информацию о MLD Snooping Querier. Конфигурация настроек отображается независимо от того, включен ли Querier на данный момент или нет.

Формат show mldsnooping querier [{detail | vlan *vlanid*}]

Режим Privileged EXEC

Если не указаны необязательные параметры *vlanid*, отображается следующая информация.

Поле	Описание
Admin Mode	Включена ли функция MLD Snooping Querier на коммутаторе.
Admin Version	Версия MLD, используемая при рассылке Query. Настройки по умолчанию: MLD v1, в настоящий момент не могут быть изменены.
Querier Address	IP-адрес, используемый в заголовке IPv6 при отправке MLD-query. Может быть настроен при помощи соответствующей команды.
Query Interval	Промежуток времени ожидания перед отправкой периодического General Query (в секундах).
Querier Timeout	Промежуток времени ожидания в состоянии Non-Querier перед переключением в состояние Querier.

Если указано значение **vlanid**, отображается следующая информация.

Поле	Описание
VLAN Admin Mode	Включена ли функция MLD Snooping Querier на данной VLAN.
VLAN Operational State	Находится ли коммутатор в состоянии “Querier” либо “Non-Querier”. Если коммутатор находится в состоянии *Querier* – он рассылает периодические General Query. Если коммутатор находится в состоянии **Non-Querier** – то query не рассылаются до тех пор, пока устройство снова не перейдет в режим «Querier».

Поле	Описание
VLAN Operational Max Response Time	Время ожидания перед удалением «Leave» с хоста после получения запроса «Leave». Это значение динамически рассчитывается из query, полученных в сети. Если коммутатор находится в состоянии Querier, то оно равно настроенному значению.
Querier Election Participate	Участвует ли данный MLD Snooping Querier в процессе выбора, в том случае если он обнаруживает присутствие во VLAN еще одного Querier.
Querier VLAN Address	IP-адрес, используемый в заголовке IPv6 при отправке MLD-query VLAN. Может быть настроен при помощи соответствующей команды.
Operational Version	Версия IPv6, используемая при рассылке query MLD в данной VLAN.
Last Querier Address	IP-адрес Querier, от которого был получен последний query.
Last Querier Version	Версия MLD последнего Querier, отправившего query в данной VLAN.

При использовании необязательного аргумента detail команда отображает глобальную информацию, а также информацию обо всех VLAN со включенным Querier.

7.24. Команды Port Security

В этом разделе описаны команды, который используется для настройки функции Port Security на коммутаторе. Функция Port Security представляет собой привязку доступных MAC-адресов к заданному порту. Пакеты, с подходящим MAC-адресом источника пересылаются нормально, а все прочие - блокируются.

ПРИМЕЧАНИЕ: Для активации SNMP trap специально для Port Security, см. “snmp-server enable traps violation”.

port-security

Данная команда активирует защиту порта на интерфейсе, диапазоне интерфейсов либо на системном уровне.

По умолчанию отключено

Формат port-security

Режим Global Config (для включения функции глобально)

Interface Config (для включения функции на интерфейсе или диапазоне интерфейсов

no port-security

Данная команда отменяет защиту порта для всех портов (Global Config) или для конкретного порта (Interface Config).

Формат no port-security

Режим Global Config

Interface Confi

port-security max-dynamic

Данная команда настраивает максимальное количество динамически привязываемых MAC-адресов для определенного порта. Диапазон: 0 – 600.

По умолчанию 600

Формат port-security max-dynamic *maxvalue*

Режим Interface Config

no port-security max-dynamic

Данная команда сбрасывает максимальное количество динамически привязываемых MAC-адресов для определенного порта на настройки по умолчанию.

Формат no port-security max-dynamic

Режим Interface Config

port-security max-static

Данная команда настраивает максимальное количество статически привязываемых MAC-адресов для определенного порта. Диапазон: 0 – 20.

По умолчанию 1

Формат port-security max-static maxvalue

Режим Interface Config

no port-security max-static

Данная команда сбрасывает максимальное количество статически привязываемых MAC-адресов для определенного порта на настройки по умолчанию.

Формат no port-security max-static

Режим Interface Config

port-security mac-address

Данная команда добавляет MAC-адрес к списку статически привязанных MAC-адресов на интерфейсе или диапазоне интерфейсов. Параметр *vid* – VLAN ID.

Формат port-security mac-address *mac-address vid*

Режим Interface Config

no port-security mac-address

Данная команда удаляет MAC-адрес из списка статически закрепленных MAC-адресов.

Формат no port-security mac-address *mac-address vid*

Режим Interface Config

port-security mac-address move

Данная команда преобразует динамически привязанный MAC-адрес в статически привязанный, для интерфейса или диапазона интерфейсов.

Формат port-security mac-address move

Режим Interface Config

port-security mac-address sticky

Данная команда активирует режим Sticky для привязки Port-MAC на порту. При указании MAC-адреса и идентификатора VLAN (только для режима Interface Config), комнада добавляет «sticky»-MAC-адрес в список статически привязанных MAC-адресов. «Sticky»-адреса преобразуются обратно в динамически привязанные при отключении режима Sticky на порту. <vid> – VLAN ID. Выполнение команды в режиме Global Config применяет режим Sticky для всех интерфейсов (физических и LAG). Глобального режима Sticky не существует.

Sticky-адреса, изученные динамически, отображаются в **show running-config** как записи “**port-security mac-address sticky <mac> <vid>**”. Это отличает их от статических записей.

Формат port-security mac-address sticky [<mac-address> <vid>]

Режим Global Config

Interface Confi

ПРИМЕР: Ниже приведен пример выполнения команды.

(Switching)(Config)# port-security mac-address sticky

(Switching)(Interface)# port-security mac-address sticky (Switching)(Interface)# port-security mac-address sticky

00:00:00:00:00:01 2

no port-security mac-address sticky

Данная команда отключает режим Sticky. Sticky-MAC-адрес может быть удален командой “**no portsecurity mac-address <mac-address> <vid>**”.

Формат no port-security mac-address sticky [<mac-address> <vid>]

Режим Global Config

Interface Confi

show port-security

Данная команда отображает параметры Port Security для порта либо портов. Если не указать параметры, команда покажет административный режим Port Security. Используйте необязательные параметры для отображения настроек для определенного интерфейса или всех интерфейсов. Для указания интерфейса LAG вместо **unit/slot/port**

можно использовать lag **lag-intf-num**. Также для определения интефейса LAG можно использовать lag **lag-intf-num**, где **lagintf-num** - номер порта LAG.

Формат show port-security [{unit/slot/port | all}]

Режим Privileged EXEC

Термин	Значение
Admin Mode	Режим привязки портов для всей системы. Это поле отображается, если не ввести ни один из дополнительных параметров.

При указании интерфейса отображается следующая информация:

Термин	Значение
Admin Mode	Режим защиты портов для интерфейса.
Dynamic Limit	Максимальное количество динамически привязанных MAC-адресов.
Static Limit	Максимальное количество статически привязанных MAC-адресов.
Violation Trap Mode	Включена ли отпрвка trap при нарушении.
Sticky Mode	Администивный режим функции Sticky на интерфейсе.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show port-security 0/1

Intf        Admin       Dynamic     Static      Violation   Sticky Trap
            Mode        Limit       Limit       Mode        Mode
-------------------------------------------------------------------------
0/1         Disabled    1           1           Disabled    Enabled
```

show port-security dynamic

Данная команда отображает динамически привязанные MAC-адреса для конкретного порта. Для указания интерфейса LAG вместо **unit/slot/port** можно использовать **lag lag-intf-num**. Также для определения интефейса LAG можно использовать lag **lag-intf-num**, где **lag-intf-num** - номер порта LAG.

Формат show port-security dynamic unit/slot/port

Режим Privileged EXEC

Термин	Значение
MAC Address	Динамически привязанный MAC-адрес.

show port-security static

Данная команда отображает статически привязанные MAC-адреса для конкретного порта. Для указания интерфейса LAG вместо **unit/slot/port** можно использовать lag **lag-intf-num**. Также для определения интефейса LAG можно использовать lag *lag-intf-num*, где **lag-intf-num** - номер порта LAG.

Формат show port-security static {unit/slot/port | lag lag-intf-num}

Режим Privileged EXEC

Термин	Значение
Statically Configured MAC Address	Статически настроенный MAC-адрес.
LAN ID	Идентификатор VLAN, содержащей хост в указанным MAC-адресом.
ticky	Указывает, была ли статическая запись MAC добавлена в режиме sticky.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show port-security static 1/0/1

Statically configured MAC Address        VLAN ID          Sticky
-------------------------------------------------------------------------
00:00:00:00:00:01                        2                Yes
00:00:00:00:00:02                        2                No

Number of static MAC addresses configured: 2
```

show port-security violation

Данная команда отображает MAC-адрес источника последнего отклоненного пакета. Для указания интерфейса LAG вместо **unit/slot/port** можно использовать **lag lag-intf-num**. Также для определения интефейса LAG можно использовать **lag lag-intf-num, где lag-intf-num** - номер порта LAG.

Формат show port-security violation {unit/slot/port | lag lag-id}

Режим Privileged EXEC

Термин	Значение
MAC Address	MAC-адрес источника последнего отклоненного фрейма.
VLAN ID	Идентификатор VLAN (если есть), связанный с MAC-адресом источника последнего отклоненного фрейма.

7.25. Команды LLDP (802.1AB)

В этом разделе описаны команды, используемые для настройки протокола LLDP (Link Layer Discovery Protocol), определенного в спецификации IEEE 802.1AB. LLDP позволяет станциям в 802 LAN объявлять основные возможности и физические описания. Данные объявления позволяют NMS (Network Management System) получать доступ к этой информации и отображать ее.

lldp transmit

Используйте эту команду для включения функции передачи LLDP для интерфейса либо диапазона интерфейсов.

По умолчанию отключено

Формат lldp transmit

Режим Interface Config

no lldp transmit

Данная команда возвращает настройкам передачи данных LLDP на значения по умолчанию.

Формат no lldp transmit

Режим Interface Config

lldp receive

Используйте эту команду для включения функции приема LLDP для интерфейса либо диапазона интерфейсов.

По умолчанию отключено

Формат lldp receive

Режим Interface Config

no lldp receive

Данная команда возвращает настройки по умолчанию для функции приема LLDPDU.

Формат no lldp receive

Режим Interface Config

lldp timers

Данная команда позволяет настроить временные параметры для передачи локальных данных на портах, на которых включена функция LLDP. Параметр *interval-seconds* определяет интервал ожидания (в секундах) между передачами LLDPDU локальных данных. Диапазон - от 5 до 32768 секунд. Параметр *hold-value* – это множитель для интервала передачи, который устанавливает TTL в LLDPDU локальных данных. Диапазон: 2 – 10. Параметр *reinit-seconds* – это задержка перед повторной инициализацией, может иметь значение в диапазоне 1-10 секунд.

По умолчанию interval—30 секунд

hold—4

reinit—2 секунды

Формат lldp timers [interval interval-seconds] [hold hold-value] [reinit reinit-seconds]

Режим Global Config

no lldp timers

Данная команда позволяет вернуть значения по умолчанию определенным параметрам тайминга для передачи локальных данных на портах, на которых включена функция LLDP.

Формат no lldp timers [interval] [hold] [reinit]

Режим Global Config

lldp transmit-tlv

Данная команда позволяет выбрать необязательные значения type length value (TLV) в базовом наборе управления 802.1AB, которые будут передаваться в LLDPDU из интерфейса или диапазона интерфейсов. Используйте **sys-name** для передачи TLV системного имени. Для настройки системного имени см. "snmp-server". Используйте **sys-desc** для передачи TLV системного описания. Используйте **sys-cap** для передачи TLV системных возможностей. Используйте **port-desc** для передачи TLV описания порта. Для настройки описания порта см. "description".

По умолчанию необязательные TLV не включены

Формат lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]

Режим Interface Config

no lldp transmit-tlv

Данная команда удаляет необязательные TLV из LLDPDU. Для удаления всех необязательных TLV используйте эту команду без параметров.

Формат no lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]

Режим Interface Config

lldp transmit-mgmt

Данная команда отключает передачу в LLDPDU информации о локальных системных управляющих адресах. Команда может использоваться для настройки как одного интерфейса, так и диапазона интерфейсов.

Формат lldp transmit-mgmt

Режим Interface Config

no lldp transmit-mgmt

Данная команда отключает передачу в LLDPDU информации о локальных системных управляющих адресах. Используйте эту команду, чтобы не включать информацию об управлении в LLDPDU.

Формат no lldp transmit-mgmt

Режим Interface Config

lldp notification

Используйте эту команду для включения уведомлений об изменении данных на интерфейсе либо диапазоне интерфейсов.

По умолчанию отключено

Формат lldp notification

Режим Interface Config

no lldp notification

Данная команда отключает уведомления.

По умолчанию отключено

Формат no lldp notification

Режим Interface Config

lldp notification-interval

Данная команда позволяет настроить частоту отправки системой уведомлений об изменении данных. Параметр *interval* – время ожидания между отправками уведомлений, в секундах. Диапазон значений: 5 – 3600 секунд.

По умолчанию 5

Формат lldp notification-interval interval

Режим Global Config

no lldp notification-interval

Данная команда возвращает настройки по умолчанию для интервала уведомлений.

Формат no lldp notification-interval

Режим Global Config

clear lldp statistics

Данная команда сбрасывает всю статистику LLDP, включая информацию, относящуюся к MED.

Формат clear lldp statistics

Режим Privileged EXEC

clear lldp remote-data

Данная команда удаляет всю информацию из таблицы удаленных данных LLDP, включая информацию, относящуюся к MED.

Формат clear lldp remote-data

Режим Global Config

show lldp

Данная команда предоставляет сводную информацию о текущей конфигурации LLDP.

Формат show lldp

Режим Privileged EXEC

Термин	Значение
Transmit Interval	Частота передачи системой локальных данных LLDPDUs, в секундах.
Transmit Hold Multiplier	Множитель для интервала передачи, который устанавливает TTL в LLDPDU локальных данных.
Re-initialization Delay	Задержка перед повторной инициализацией, в секундах.
Notification Interval	Частота передачи системой уведомлений об изменении локальных данных, в секундах.

show lldp interface

Данная команда предоставляет сводную информацию о текущей конфигурации LLDP для указанного интерфейса или для всех интерфейсов.

Формат show lldp interface {unit/slot/port | all}

Режим Privileged EXEC

Термин	Значение
Interface	Интерфейс в формате *unit/slot/port*.
Link	Информация о состоянии линка.

Термин	Значение
Transmit	Передает ли интерфейс LLDPDU.
Receive	Принимает ли интерфейс LLDPDU.
Notify	Отправляет ли интерфейс уведомления об изменении данных.
TLVs	Отправляет ли интерфейс необязательные TLV в LLDPDU. Коды TLV могут быть: 0 (описание порта), 1 (системное имя), 2 (описание системы) либо 3 (возможности системы).
Mgmt	Передает ли интерфейс информацию об адресах системного управления в LLDPDU.

show lldp statistics

Данная команда предоставляет информацию о текущем трафике LLDP и статистике удаленной таблицы удаленной статистики для указанного интерфейса или для всех интерфейсов.

Формат show lldp statistics {unit/slot/port | all}

Режим Privileged EXEC

Термин	Значение
Last Update	Время, прошедшее с последнего обновления удаленной таблицы, в днях, часах, минутах и секундах.
Total Inserts	Суммарное количество вставок удаленную таблицу данных.
Total Deletes	Суммарное количество удалений из удаленной таблицы данных.
Total Drops	Суммарное количество раз, когда полные удаленные данные были приняты, но не были вставлены по причине нехватки ресурсов.
Total Ageouts	Суммарное количество раз, когда полные удаленные данные были удалены по причине истечения TTL.

Таблица содержит следующие заголовки столбцов:

Термин	Значение
Interface	Интерфейс в формате *unit/slot/port*.
TX Total	Общее количество пакетов LLDP, переданных портом.

Термин	Значение
RX Total	Общее количество пакетов LLDP, полученных портом.
Discards	Общее количество фреймов LLDP, отклоненных портом по тем или иным причинам.
Errors	Количество поврежденных фреймов LLDP, полученных на порте.
Ageouts	Суммарное количество раз, когда полные удаленные данные были удалены для этого порта по причине истечения TTL.
TVL Discards	Количество отброшенных TLV.
TVL Unknowns	Общее количество LLDP TLV, полученных на порте, где значение типа принадлежал к зарезервированному диапазону и не был распознан.
TLV MED	Общее количество LLDP-MED TLV, полученных на интерфейсе.
TLV 802.1	Общее количество LLDP TLV, полученных на интерфейсе типа 802.1.
TLV 802.3	Общее количество LLDP TLV, полученных на интерфейсе типа 802.3.

show lldp remote-device

Данная команда отображает сводную информацию об удаленных устройствах, передающих текущие данные LLDP в систему. Команда может выводить информацию как для всех портов, так и отдельно для указанного порта.

Формат show lldp remote-device {unit/slot/port | all}

Режим Privileged EXEC

Термин	Значение
Local Interface	Интерфейс, получивший LLDPDU с удаленного устройства.
RemID	Внутренний идентификатор, используемый коммутатором для маркировки каждого удаленного устройства в системе.
Chassis ID	Идентификатор, отправляемый удаленным устройством в качестве части сообщения LLDP (как правило, представляет собой MAC-адрес устройства).
Port ID	Номер порта, передавшего LLDPDU.

Термин	Значение
System Name	Системное имя удаленного устройства.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Switching) #show lldp remote-device all
LLDP Remote Device Summary
Local Interface  RemID  Chassis ID          Port ID             System Name
0/1
0/2
0/3
0/4
0/5
0/6
0/7              2      00:FC:E3:90:01:0F   00:FC:E3:90:01:11
0/7              3      00:FC:E3:90:01:0F   00:FC:E3:90:01:12
0/7              4      00:FC:E3:90:01:0F   00:FC:E3:90:01:13
0/7              5      00:FC:E3:90:01:0F   00:FC:E3:90:01:14
0/7              1      00:FC:E3:90:01:0F   00:FC:E3:90:03:11
0/7              6      00:FC:E3:90:01:0F   00:FC:E3:90:04:11
0/8
0/9
0/10
0/11
0/12
--More-- or (q)uit
```

show lldp remote-device detail

Данная команда отображает детальную информацию об удаленных устройствах, передающих текущие LLDP данные на интерфейс в системе.

Формат show lldp remote-device detail unit/slot/port

Режим Privileged EXEC

Термин	Значение
Local Interface	Интерфейс, получивший LLDPDU с удаленного устройства.
Remote Identifier	Внутренний идентификатор, используемый коммутатором для маркировки каждого удаленного устройства в системе.
Chassis ID Subtype	Тип идентификации, используемый в поле Chassis ID.
Chassis ID	ID удаленного устройства.
Port ID Subtype	Тип порта на удаленном устройстве.
Port ID	Номер порта, передавшего LLDPDU.
System Name	Системное имя удаленного устройства.
System Description	Описание удаленный системы, включающее в себя системное имя, версию оборудования, операционную систему, а также сетевое ПО, поддерживаемое устройством.
Port Description	Описание порта в буквенно-цифровом формате. Описание порта можно настроить.
System Capabilities Supported	Указывает основную функнциональность устройства.
System Capabilities Enabled	Указывает, какие из поддерживаемых функций системы находятся во включенном состоянии.
Management Address	Для каждого интерфейса удаленного устройства с агентом LLDP сообщается используемый агентом тип адреса, а также адрес, используемый для получения относящейся к этому устройству информации.
Time To Live	Время в секундах, в течение которого информация, полученная в LLDPDU, должна рассматриваться как актуальная.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Switching) #show lldp remote-device detail 0/7
LLDP Remote Device Detail
Local Interface: 0/7
Remote Identifier: 2
Chassis ID Subtype: MAC Address
```

Chassis ID: 00:FC:E3:90:01:0F

Port ID Subtype: MAC Address Port ID: 00:FC:E3:90:01:11

System Name:

System Description:

Port Description:

System Capabilities Supported:

System Capabilities Enabled: Time to Live: 24 seconds

show lldp local-device

Данная команда отображает информацию о локальных данных, объявляемых LLDP. Команда может отображать сводную информацию, либо показывать детальную информацию для каждого интерфейса.

Формат show lldp local-device {unit/slot/port | all}

Режим Privileged EXEC

Термин	Значение
Interface	Интерфейс в формате unit/slot/port.
Port ID	Идентификатор порта, связанный с этим интерфейсом.
Port Description	Описание порта, связанное с этим интерфейсом.

show lldp local-device detail

Данная команда отображает детальную информацию о данных LLDP, передаваемых указанным интерфейсом.

Формат show lldp local-device detail unit/slot/port

Режим Privileged EXEC

Термин	Значение
Interface	Интерфейс, отправляющий LLDPDU.
Chassis ID Subtype	Тип идентификации, используемый в поле Chassis ID.
Chassis ID	ID локального устройства.
Port ID Subtype	Тип порта на локальном устройстве.
Port ID	Номер порта, передающего LLDPDU.

Термин	Значение
System Name	Системное имя локального устройства.
System Description	Описание локальной системы, включающее в себя системное имя, версию оборудования, операционную систему, а также сетевое ПО, поддерживаемое устройством.
Port Description	Описание порта в буквенно-цифровом формате.
System Capabilities Supported	Указывает основную функнциональность устройства.
System Capabilities Enabled	Указывает, какие из поддерживаемых функций системы находятся во включенном состоянии.
Management Address	Тип адреса и сам адрес, используемые локальным LLDP-агентом для приёма и передачи информации.

7.26. Команды LLDP-MED

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) (ANSI-TIA-1057) представляет собой расширение стандарта LLDP. В частности, LLDP-MED предоставляет расширения для настройки и политики сети, расположения устройств, Power over Ethernet (PoE) и управления ресурсами.

lldp med

Данная команда позволяет включить MED на интерфейсе либо диапазоне интерфейсов. Включив MED, вы автоматически активируете принимающий и передающий функционал LLDP.

По умолчанию отключено

Формат lldp med

Режим Interface Config

no lldp med

Данная команда отключает MED.

Формат no lldp med

Режим Interface Config

lldp med confignotification

Данная команда настраивает интерфейс или диапазон интерфейсов на отправку уведомлений об изменении топологии.

По умолчанию отключено

Формат lldp med confignotification

Режим Interface Config

no lldp med confignotification

Данная команда отключает уведомления.

Формат no lldp med confignotification

Режим Interface Config

lldp med transmit-tlv

Данная команда позволяет выбрать необязательные значения type length value (TLV) в наборе LLDP MED, которые будут передаваться в LLDPDU из интерфейса или диапазона интерфейсов. Набор доступных параметров определяется типом устроства.

По умолчанию По умолчанию включены TLV возможностей и сетевой политики.

Формат lldp med transmit-tlv [capabilities] [ex-pse] [network-policy]

Режим Interface Config

Термин	Значение
capabilities	Передает TLV возможностей LLDP.
ex-pd	Передает TLV расширенного PD LLDP
ex-pse	Передает TLV расширенного PSE LLDP.
inventory	Передает TLV ресурсов LLDP.
location	Передает TLV местонахождения LLDP.
network-policy	Передает TLV сетевой политики LLDP.

no lldp med transmit-tlv

Данная команда удаляет TLV.

Формат no lldp med transmit-tlv [capabilities] [ex-pse] [network-policy]

Режим Interface Config

lldp med all

Данная команда используется для настройки LLDP-MED на всех портах.

Формат lldp med all

Режим Global Config

lldp med confignotification all

Данная команда настраивает все порты на отправку уведомлений об изменении топологии.

Формат lldp med confignotification all

Режим Global Config

lldp med faststartrepeatcount

Данная команда позволяет установить значение количества повторов быстрого запуска. *[count]* – это количество LLDP PDU, которые будут отправлены после включения продукта. Диапазон - от 1 до 10.

По умолчанию 3

Формат lldp med faststartrepeatcount [count]

Режим Global Config

no lldp med faststartrepeatcount

Данная команда возвращает значения по умолчанию.

Формат no lldp med faststartrepeatcount

Режим Global Config

lldp med transmit-tlv all

Данная команда позволяет выбрать необязательные значения type length value (TLV) в наборе LLDP MED, которые будут передаваться в LLDPDU. Набор доступных параметров определяется типом устроства.

По умолчанию включены TLV возможностей и сетевой политики.

Формат lldp med transmit-tlv all [capabilities] [network-policy]

Режим Global Config

Термин	Значение
capabilities	Передает TLV возможностей LLDP.
ex-pd	Передает TLV расширенного PD LLDP
ex-pse	Передает TLV расширенного PSE LLDP.
inventory	Передает TLV ресурсов LLDP.
location	Передает TLV местонахождения LLDP.
network-policy	Передает TLV сетевой политики LLDP.

no lldp med transmit-tlv

Данная команда удаляет TLV.

Формат no lldp med transmit-tlv [capabilities] [network-policy]

Режим Global Config

show lldp med

Данная команда предоставляет сводную информацию о текущей конфигурации LLDP MED.

Формат show lldp med

Режим Privileged EXEC

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show lldp med

LLDP MED Global Configuration

Fast Start Repeat Count: 3

Device Class: Network Connectivity

(Routing) #
```

show lldp med interface

Данная команда предоставляет сводную информацию о текущей конфигурации LLDP MED для определенного интерфейса. **unit/slot/port** – определенный физический интерфейс. **all** – все действительные интерфейсы LLDP.

Формат show lldp med interface {unit/slot/port | all}

Режим Privileged EXEC

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show lldp med interface all
```

Interface	Link	configMED	operMED	ConfigNotify	TLVsTx
1/0/1	Down	Disabled	Disabled	Disabled	0,1
1/0/2	Up	Disabled	Disabled	Disabled	0,1
1/0/3	Down	Disabled	Disabled	Disabled	0,1
1/0/4	Down	Disabled	Disabled	Disabled	0,1
1/0/5	Down	Disabled	Disabled	Disabled	0,1
1/0/6	Down	Disabled	Disabled	Disabled	0,1
1/0/7	Down	Disabled	Disabled	Disabled	0,1
1/0/8	Down	Disabled	Disabled	Disabled	0,1
1/0/9	Down	Disabled	Disabled	Disabled	0,1
1/0/10	Down	Disabled	Disabled	Disabled	0,1
1/0/11	Down	Disabled	Disabled	Disabled	0,1

1/0/12	Down	Disabled	Disabled	Disabled	0,1
1/0/13	Down	Disabled	Disabled	Disabled	0,1
1/0/14	Down	Disabled	Disabled	Disabled	0,1

TLV Codes: 0 - Capabilities 1 - Network Policy
2 - Location 3 - Extended PSE
4 - Extended Pd 5 - Inventory
--More-- or (q)uit

(Routing) #show lldp med interface 1/0/2

Interface	Link	configMED	operMED	ConfigNotify	TLVsTx
1/0/2	Up	Disabled	Disabled	Disabled	0,1

TLV Codes: 0 - Capabilities 1 - Network Policy
2 - Location 3 - Extended PSE
4 - Extended Pd 5 - Inventory
(Routing) #

show lldp med local-device detail

Данная команда отображает детальную информацию о данных LLDP MED, передаваемых указанным интерфейсом. unit/slot/port – определенный физический интерфейс.

Формат show lldp med local-device detail unit/slot/port

Режим Privileged EXEC

ПРИМЕР: Вывод командной строки для данной команды.

(Routing) # show lldp med local-device detail 1/0/8
LLDP MED Local Device Detail
Interface: 1/0/8
Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True

Media Policy Application Type : streamingvideo

Vlan ID: 20

Priority: 1

DSCP: 2

Unknown: False Tagged: True

Inventory

Hardware Rev: xxx xxx xxx

Firmware Rev: xxx xxx xxx

Software Rev: xxx xxx xxx

Serial Num: xxx xxx xxx Mfg Name: xxx xxx xxx

Model Name: xxx xxx xxx

Asset ID: xxx xxx xxx

Location

Subtype: elin

Info: xxx xxx xxx

Extended POE

Device Type: pseDevice

Extended POE PSE

Available: 0.3 Watts

Source: primary

Priority: critical

Extended POE PD

Required: 0.2 Watts

Source: local

Priority: low

show lldp med remote-device

Данная команда отображает сводную информацию об удаленных устройствах, передающих текущие данные LLDP MED в систему. Команда может выводить информацию об удаленных данных LLDP MED, полученных как на всех действительных интерфейсах LLDP, так и на указанном физическом интерфейсе.

Формат show lldp med remote-device {unit/slot/port | all}

Режим Privileged EXEC

Термин	Значение
Local Interface	Интерфейс, получивший LLDPDU с удаленного устройства.

Термин	Значение
Remote ID	Внутренний идентификатор, используемый коммутатором для маркировки каждого удаленного устройства в системе.
Device Class	Класс удаленного устройства.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show lldp med remote-device all
LLDP MED Remote Device Summary
Local
Interface                Remote ID          Device Class
-------------------------------------------------------------------------
1/0/8                    1                  Class I
1/0/9                    2                  Not Defined
1/0/10                   3                  Class II
1/0/11                   4                  Class III
1/0/12                   5                  Network Con
```

show lldp med remote-device detail

Данная команда отображает детальную информацию об удаленных устройствах, передающих текущие данные LLDP MED на интерфейс в системе.

Формат show lldp med remote-device detail unit/slot/port

Режим Privileged EXEC

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show lldp med remote-device detail 1/0/8
LLDP MED Remote Device Detail
Local Interface: 1/0/8
Remote Identifier: 18
Capabilities
MED Capabilities Supported: capabilities, networkpolicy, location, extendedpse
MED Capabilities Enabled: capabilities, networkpolicy
Device Class: Endpoint Class I
Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
DSCP: 1
```

Unknown: False

Tagged: True

Media Policy Application Type : streamingvideo

Vlan ID: 20

Priority: 1

DSCP: 2

Unknown: False Tagged: True

Inventory

Hardware Rev: xxx xxx xxx

Firmware Rev: xxx xxx xxx

Software Rev: xxx xxx xxx

Serial Num: xxx xxx xxx Mfg Name: xxx xxx xxx

Model Name: xxx xxx xxx Asset ID: xxx xxx xxx

Location

Subtype: elin

Info: xxx xxx xxx

Extended POE

Device Type: pseDevice

Extended POE PSE

Available: 0.3 Watts

Source: primary

Priority: critical

Extended POE PD

Required: 0.2 Watts

Source: local

Priority: low

7.27. Команды Denial of Service

В этом разделе описаны команды, используемые для настройки функции защиты от DoS-атак (Denial of Service). ПО коммутатора позволяет классифицировать и блокировать DoS-атаки определенных типов. Вы можете настроить систему на блокирование следующих типов атак:

- SIP = DIP: IP-адрес источника = IP-адрес назначения.
- First Fragment: TCP-заголовок меньший чем настроенное значение.
- TCP Fragment: Позволяет устройству отбрасывать пакеты, имеющие такой объем полезных данных TCP, при котором значение объема полезных данных IP минус размер IP-заголовка меньше, чем минимально допустимый объем заголовка TCP.

- TCP Flag: TCP-флаг SYN настроен и Порт источника < 1024, либо TCP Control Flags = 0 и TCP Sequence Number = 0, либо TCP-флаги FIN, URG, и PSH настроены и TCP Sequence Number = 0, либо настроены TCP-флаги SYN и FIN.
- L4 Port: TCP/UDP-порт источника = TCP/UDP-порт назначения.
- ICMP: Ограничение размера пакетов ICMP Ping.

ПРИМЕЧАНИЕ: Поддержка отслеживания и блокировки типов атак, может отличаться в зависимости от модели устройства.

- SMAC = DMAC: MAC-адрес источника = MAC-адрес назначения.
- TCP Port: TCP-порт источника = TCP-порт назначения
- UDP Port: UDP-порт источника = UDP-порт назначения
- TCP Flag & Sequence: TCP-флаг SYN настроен и Порт источника < 1024, либо TCP Control Flags = 0 и TCP Sequence Number = 0, либо TCP-флаги FIN, URG, и PSH настроены и TCP Sequence Number = 0, либо TCP-флаги SYN и FIN настроены.
- TCP Offset: Позволяет устройству отбрасывать пакеты, имеющие Offset заголовка TCP, равный 1.
- TCP SYN: Настроенный TCP-флаг SYN.
- TCP SYN & FIN: Настроенные TCP-флаги SYN и FIN.
- TCP FIN & URG & PSH: Настроенные TCP-флаг FIN, URG и PSH, и TCP Sequence Number = 0.
- ICMP V6: Ограничение размера пакетов ICMPv6 Ping.
- ICMP Fragment: Проверка на фрагментированные пакеты ICMP.

dos-control all

Данная команда включает функцию защиты от DoS-атак глобально.

По умолчанию отключено

Формат dos-control all

Режим Global Config

no dos-control all

Данная команда глобально отключает функцию защиты от DoS-атак.

Формат no dos-control all

Режим Global Config

dos-control sipdip

Данная команда включает защиту от DoS-атак типа IP-адрес источника = IP-адрес назначения (SIP=DIP). Если этот режим включен, функция защиты от DoS-атак начинает противодействовать атакам этого типа. При включении данного режима система будет отбрасывать входящие пакеты с SIP=DIP.

По умолчанию отключено

Формат dos-control sipdip

Режим Global Config

no dos-control sipdip

Данная команда отключает защиту от DoS-атак типа SIP=DIP.

Формат no dos-control sipdip

Режим Global Config

dos-control firstfrag

Данная команда включает защиту от DoS-атак типа «Minimum TCP Header Size» (минимальный размер TCP-заголовка). Если этот режим включен, функция защиты от DoS-атак начинает противодействовать атакам этого типа. Если входящий пакет имеет объем заголовка TCP меньше настроенного значения, то этот пакет будет отброшен. Режим отключен по умолчанию. Если вы включите этот режим, но не установите минимальный размер заголовка, система установит это значение на 20.

По умолчанию отключено (20)

Формат dos-control firstfrag [0-255]

Режим Global Config

no dos-control firstfrag

Данная команда выключает режим проверки минимального размера TCP-заголовка.

Формат no dos-control firstfrag

Режим Global Config

dos-control tcpfrag

Данная команда включает защиту от DoS-атак типа «TCP Fragment». Если этот режим включен, система будет обрасывать все пакеты, имеющие объем полезного содержания TCP, в котором объем полезного содержания IP минус длина заголовка составляют меньшую величину, нежели минимально допустимый объем TCP-заголовка.

По умолчанию отключено

Формат dos-control tcpfrag

Режим Global Config

no dos-control tcpfrag

Данная команда отключает защиту от DoS-атак типа «TCP Fragment Denial».

Формат no dos-control tcpfrag

Режим Global Config

dos-control tcpflag

Данная команда включает защиту от DoS-атак типа «TCP Flag». Если этот режим включен, функция защиты от DoS-атак начинает противодействовать атакам этого типа. Если этот режим включен, отбрасываются входящие пакеты с установленным значением TCP Flag SYN и порт источника меньше 1024, или установлены флаги TCP Control, равные 0, а TCP Sequence Number установлен на 0 или установлены флаги TCP FIN, URG и PSH и TCP Sequence Number, установленный в 0 или имеющие Флаги TCP SYN и FIN.

По умолчанию отключено

Формат dos-control tcpfrag

Режим Global Config

no dos-control tcpflag

Данная команда отключает защиту от DoS-атак типа «TCP Flag».

Формат no dos-control tcpfrag

Режим Global Config

dos-control l4port

Данная команда включает защиту от DoS-атак типа « L4 Port». Если этот режим включен, функция защиты от DoS-атак начинает противодействовать атакам этого типа. Если этот режим включен, отбрасываются входящие пакеты, имеющие номер порта источника TCP/UDP, равный номеру порта назначения TCP/UDP.

ПРИМЕЧАНИЕ: Некоторые приложения используют одни и те же порты L4 и в качестве назначения, и в качестве источника. Например, протокол RIP использует номер порта 520 для обоих случаев. При использовании такой меры защиты от DoS-атак, как l4port, приложения RIP могут терять пакеты, что может привести к прекращению работы приложений.

По умолчанию отключено

Формат dos-control l4port

Режим Global Config

no dos-control l4port

Данная команда включает защиту от DoS-атак типа «L4 Port».

Формат no dos-control l4port

Режим Global Config

dos-control smacdmac

ПРИМЕЧАНИЕ: Поддержка данной команды зависит от модели устройства.

Данная команда включает защиту от DoS-атак типа «MAC address = Destination MAC» (SMAC=DMAC). Если этот режим включен, функция защиты от DoS-атак начинает противодействовать атакам этого типа. При включении данного режима система будет отбрасывать входящие пакеты с SMAC=DMAC.

По умолчанию отключено

Формат dos-control smacdmac

Режим Global Config

no dos-control smacdmac

Данная команда включает защиту от DoS-атак типа SMAC=DMAC.

Формат no dos-control smacdmac

Режим Global Config

dos-control tcpport

ПРИМЕЧАНИЕ: Поддержка данной команды зависит от модели устройства..

Данная команда включает защиту от DoS-атак типа «Source TCP Port = Destination TCP Port».

Если этот режим включен, функция защиты от DoS-атак начинает противодействовать атакам этого типа. Если этот режим включен, отбрасываются входящие пакеты, имеющие одинаковый номер портов источника и назначения.

По умолчанию отключено

Формат dos-control tcpport

Режим Global Config

no dos-control tcpport

Данная команда отключает защиту от DoS-атак типа «Source TCP Port = Destination TCP Port».

Формат no dos-control tcpport

Режим Global Config

dos-control udpport

ПРИМЕЧАНИЕ: Поддержка данной команды зависит от модели устройства.

Данная команда включает защиту от DoS-атак типа «Source UDP Port = Destination UDP Port». Защита. Если этот режим включен, функция защиты от DoS-атак начинает противодействовать атакам этого типа. Если этот режим включен, отбрасываются входящие пакеты, имеющие одинаковый номер портов источника и назначения.

По умолчанию отключено

Формат dos-control udpport

Режим Global Config

no dos-control udpport

Данная команда отключает защиту от DoS-атак типа «Source UDP Port = Destination UDP Port».

Формат no dos-control udpport

Режим Global Config

dos-control tcpflagseq

ПРИМЕЧАНИЕ: Поддержка данной команды зависит от модели устройства..

Данная команда включает защиту от DoS-атак типа « TCP Flag and Sequence». Если этот режим включен, функция защиты от DoS-атак начинает противодействовать атакам этого типа. Если этот режим включен, отбрасываются входящие пакеты с установленным значением TCP Flag SYN и порт источника меньше 1024, или установлены флаги TCP Control, равные 0, а TCP Sequence Number установлен на 0 или установлены флаги TCP FIN, URG и PSH и TCP Sequence Number установленный в 0, или имеющий Флаги TCP SYN и FIN.

По умолчанию отключено

Формат dos-control tcpflagseq

Режим Global Config

no dos-control tcpflagseq

Данная команда отключает защиту от DoS-атак типа «TCP Flag and Sequence».

Формат no dos-control tcpflagseq

Режим Global Config

dos-control tcpoffset

ПРИМЕЧАНИЕ: Поддержка данной команды зависит от модели устройства.

Данная команда включает защиту от DoS-атак типа «TCP offset». Если этот режим включен, функция защиты от DoS-атак начинает противодействовать атакам этого типа. При включении данного режима система будет отбрасывать входящие пакеты со смещением заголовка TCP, равным единице (1).

По умолчанию отключено

Формат dos-control tcpoffset

Режим Global Config

no dos-control tcpoffset

Данная команда отключает защиту от DoS-атак типа «TCP offset».

Формат no dos-control tcpoffset

Режим Global Config

dos-control tcpsyn

ПРИМЕЧАНИЕ: Поддержка данной команды зависит от модели устройства.

Данная команда включает защиту от DoS-атак типа «TCP SYN and L4 source = 0-1023». Если этот режим включен, функция защиты от DoS-атак начинает противодействовать

атакам этого типа. При включении данного режима система будет отбрасывать входящие пакеты с настроенным TCP-флагом SYN и портом источника L4 от 0 до 1023.

По умолчанию отключено

Формат dos-control tcpsyn

Режим Global Config

no dos-control tcpsyn

Данная команда отключает защиту от DoS-атак типа «TCP SYN and L4 source = 0-1023».

Формат no dos-control tcpsyn

Режим Global Config

dos-control tcpsynfin

ПРИМЕЧАНИЕ: Поддержка данной команды зависит от модели устройства.

Данная команда включает защиту от DoS-атак типа «TCP SYN and FIN». Если этот режим включен, функция защиты от DoS-атак начинает противодействовать атакам этого типа. При включении данного режима система будет отбрасывать входящие пакеты с настроенными TCP-флагами SYN и FIN.

По умолчанию отключено

Формат dos-control tcpsynfin

Режим Global Config

no dos-control tcpsynfin

Данная команда отключает защиту от DoS-атак типа «TCP SYN & FIN».

Формат no dos-control tcpsynfin

Режим Global Config

dos-control tcpfinurgpsh

ПРИМЕЧАНИЕ: Поддержка данной команды зависит от модели устройства.

Данная команда включает защиту от DoS-атак типа «TCP FIN, URG, PSH and SEQ = 0». Если этот режим включен, функция защиты от DoS-атак начинает противодействовать атакам этого типа. При включении данного режима система будет отбрасывать входящие пакеты с настроенными флагами TCP FIN, URG и PSH, и с TCP Sequence Number настроенным на 0.

По умолчанию отключено

Формат dos-control tcpfinurgpsh

Режим Global Config

no dos-control tcpfinurgpsh

Данная команда отключает защиту от DoS-атак типа «TCP FIN, URG, PSH and SEQ = 0».

Формат no dos-control tcpfinurgpsh

Режим Global Config

dos-control icmpv4

ПРИМЕЧАНИЕ: Поддержка данной команды зависит от модели устройства.

Данная команда включает защиту от DoS-атак типа «Maximum ICMPv4 Packet Size». Если этот режим включен, функция защиты от DoS-атак начинает противодействовать атакам этого типа. При включении данного режима система будет отбрасывать входящие пакеты ICMPv4 Echo Request (PING) с размером больше настроенного значения.

По умолчанию отключено (512)

Формат dos-control icmpv4 [0-16376]

Режим Global Config

no dos-control icmpv4

Данная команда отключает защиту от DoS-атак типа «Maximum ICMP Packet Size».

Формат no dos-control icmpv4

Режим Global Config

dos-control icmpv6

ПРИМЕЧАНИЕ: Поддержка данной команды зависит от модели устройства

Данная команда включает защиту от DoS-атак типа «Maximum ICMPv6 Packet Size». Если этот режим включен, функция защиты от DoS-атак начинает противодействовать атакам этого типа. При включении данного режима система будет отбрасывать входящие пакеты ICMPv6 Echo Request (PING) с размером больше настроенного значения.

По умолчанию отключено (512)

Формат dos-control icmpv6 0-16376

Режим Global Config

no dos-control icmpv6

Данная команда отключает защиту от DoS-атак типа «Maximum ICMP Packet Size».

Формат no dos-control icmpv6

Режим Global Config

dos-control icmpfrag

ПРИМЕЧАНИЕ: Поддержка данной команды зависит от модели устройства.

Данная команда включает защиту от DoS-атак типа «ICMP Fragment». Если этот режим включен, функция защиты от DoS-атак начинает противодействовать атакам этого типа. При включении данного режима система будет отбрасывать фрагментированные входящие пакеты ICMP.

По умолчанию отключено

Формат dos-control icmpfrag

Режим Global Config

no dos-control icmpfrag

Данная команда отключает защиту от DoS-атак типа «ICMP Fragment».

Формат no dos-control icmpfrag

Режим Global Config

show dos-control

Данная команда предоставляет информацию о настройках функции защиты от DoS-атак.

Формат show dos-control

Режим Privileged EXEC

ПРИМЕЧАНИЕ: Отображение некоторых из нижеприведенных пунктов зависит от модели устройства.

Термин	Значение
First Fragment Mode	Административный режим защиты «First Fragment». При включении коммутатор отбрасывает пакеты, объем TCP-заголовков которых меньше настроенного значения Min TCP Hdr Size.
Min TCP Hdr Size	Минимальный объем заголовка TCP, который принимается коммутатором при включенной защите First Fragment.
ICMPv4 Mode	Административный режим защиты «ICMPv4». При включении коммутатор отбрасывает ICMP-пакеты, имеющие тип ECHO_REQ (ping) и объем больше настроенного значения ICMPv4 Payload Size.
Max ICMPv4 Payload Size	Максимальный полезный объем ICMPv4, принимаемый при включении защиты ICMPv4.
ICMPv6 Mode	Административный режим защиты «ICMPv6». При включении коммутатор отбрасывает ICMP-пакеты, имеющие тип ECHO_REQ (ping) и объем больше настроенного значения ICMPv6 Payload Size.
Max ICMPv6 Payload Size	Максимальный полезный объем ICMPv6, принимаемый при включении защиты ICMPv6.
ICMPv4 Fragment Mode	Административный режим защиты «ICMPv4 Fragment». При включении коммутатор отбрасывает фрагментированные ICMPv4-пакеты

Термин	Значение
TCP Port Mode	Административный режим защиты «TCP Port». При включении коммутатор отбрасывает пакеты, у которых совпадают номера TCP-портов источника и назначения.
UDP Port Mode	Административный режим защиты «UDP Port». При включении коммутатор отбрасывает пакеты, у которых совпадают номера UDP-портов источника и назначения.
SIPDIP Mode	Административный режим защиты «UDP= DIP». При включении коммутатор отбрасывает пакеты у которых совпадают IP-адреса источника и назначения. По умолчанию - выключен.
SMACDMAC Mode	Административный режим защиты «SMAC=DMAC». При включении коммутатор отбрасывает пакеты у которых совпадают MAC-адреса источника и назначения.
TCP FIN&URG& PSH Mode	Административный режим защиты «TCP FIN & URG & PSH». При включении данного режима система будет отбрасывать входящие пакеты с настроенными флагами TCP FIN, URG и PSH, и с TCP Sequence Number настроенным на 0.
TCP Flag & Sequence Mode	Административный режим защиты «TCP Flag». При включении данного режима система будет отбрасывать входящие пакеты с управляющими флагами TCP, настроенными на 0, и с TCP Sequence Number, настроенным на 0.
TCP SYN Mode	Административный режим защиты «TCP SYN». При включении данного режима система будет отбрасывать входящие пакеты с настроенными флагами TCP SYN.
TCP SYN & FIN Mode	Административный режим защиты «TCP SYN & FIN». При включении данного режима система будет отбрасывать входящие пакеты с настроенными флагами TCP SYN и FIN.
TCP Fragment Mode	Административный режим защиты «TCP Fragment». При включении данного режима система будет отбрасывать входящие пакеты, имеющие такой объем полезных данных TCP, при котором значение объема полезных данных IP минус размер IP-заголовка меньше, чем минимально допустимый объем заголовка TCP.
TCP Offset Mode	Административный режим защиты «TCP Offset». При включении данного режима система будет отбрасывать входящие пакеты, имеющие сдвиг заголовка TCP, настроенный на 1.

7.28. Команды базы данных MAC

В этом разделе описаны команды, используемые для настройки и просмотра информации о базах данных MAC-адресов.

bridge aging-time

Данная команда настраивает время устаревания адресов для базы данных пересылки (в секундах). Значение *seconds* - целое число в диапазоне 10 - 1 000 000.

По умолчанию 300

Формат bridge aging-time 10-1,000,000

Режим Global Config

no bridge aging-time

Данная команда сбрасывает значение времени устаревания адресов для базы данных пересылки на значение по умолчанию.

Формат no bridge aging-time

Режим Global Config

show forwardingdb agetime

Данная команда отображает значение времени устаревания адресов.

По умолчанию All

Формат show forwardingdb agetime

Режим Privileged EXEC

Термин	Значение
Address Aging Timeout	Отображает значение времени устаревания адресов, в секундах.

show mac-address-table multicast

Данная команда отображает информацию о MFDB (Multicast Forwarding Database). При вводе команды без параметров будет отображена вся таблица. Вы также можете вывести данные для одного MAC-адреса, указав его в виде необязательного параметра.

Формат show mac-address-table multicast *macaddr*

Режим Privileged EXEC

Термин	Значение
VLAN ID	VLAN, в которой изучен MAC-адрес.

Термин	Значение
MAC Address	MAC-адрес, для которого коммутатор имеет информацию о перенаправлении или фильтрации. Формат - 6 двухзначных шестнадцатеричных чисел, разделенных двоеточиями, например 01:23:45:67:89:AB.
Source	Компонент, ответственный за данную запись в Multicast Forwarding Database. Значение может быть одним из следующих: IGMP Snooping, GMRP или Static Filtering.
Type	Тип записи. Статические записи сгенерирвоаны конечным пользователем. Динамические – добавлены в таблицу в результате процесса обучения протокола.
Description	Текстовое описание записи.
Interfaces	Список интерфейсов, предназначенных для перенаправления (Fwd:) и фильтрации (Flt:).
Fwd Interface	Полученный список передачи получается из объединения всех интерфейсов передачи со всех компонентов, за вычетом интерфейсов, которые перечислены как интерфейсы статической фильтрации.

ПРИМЕР: Если таблица переадресации содержит одну или более записей, вывод команды выглядит похожим образом:

```
(Routing) #show mac-address-table multicast

Fwd   VLAN ID MAC Address       Source    Type      Description   Interface   Interface
                                                                  
------------------------------------------------------------------------------------
1     01:00:5E:01:02:03         Filter    Static    Mgmt Config   Fwd:        Fwd:
                                                                  1/0/1       1/0/1
                                                                  1/0/2       1/0/2
                                                                  1/0/3       1/0/3
                                                                  1/0/4       1/0/4
                                                                  1/0/5       1/0/5
                                                                  1/0/6       1/0/6
                                                                  1/0/7       1/0/7
                                                                  1/0/8       1/0/8
                                                                  1/0/9       1/0/9
```

```
                                                    1/0/10          1/0/10
--More-- or (q)uit
```

show mac-address-table stats

Данная команда отображает статистику MFDB (Multicast Forwarding Database).

Формат show mac-address-table stats

Режим Privileged EXEC

Термин	Значение
Total Entries	Общее количество записей, которое может поддерживать таблица MFDB.
Most MFDB Entries Ever Used	Наибольшее количество записей, которое присутствовало в таблице MFDB.
Current Entries	Текущее количество записей в MFDB.

8. КОМАНДЫ МАРШРУТИЗАЦИИ

В этом разделе описываются команды маршрутизации.

Раздел состоит из следующих глав:

ВНИМАНИЕ: В ДАННОМ РАЗДЕЛЕ КОМАНДЫ ДЕЛЯТСЯ НА ТРИ ФУНКЦИОНАЛЬНЫЕ ГРУППЫ:

1. Команды Show отображают настройки коммутатора, статистику и прочую информацию.
2. Команды конфигурации вносят изменения в настройки коммутатора. Каждой команде конфигурации соответствует команда информации, показывающая текущие настройки.
3. Команды Clear сбрасывают определенные настройки на заводские значения.

8.1. Команды Address Resolution Protocol

В этом разделе описаны команды, который используется для конфигурации ARP (Address Resolution Protocol) и просмотра информации, касающейся ARP. Протокол ARP ассоциирует IP-адреса с MAC-адресами, и хранит эту информацию в виде ARP-записей в ARP-кэше.

arp

Данная команда создает запись ARP. Значение **ipaddress** - это IP-адрес устройства в подсети, подключенной к существующему интерфейсу маршрутизации. Параметр **macaddr** является одноадресным MAC-адресом этого устройства. Параметр «**interface**» задает интерфейс следующего перехода.

Формат - 6 двухзначных шестнадцатеричных чисел, разделенных двоеточиями, например 00:06:29:32:81:40.

Формат arp ipaddress macaddr interface {unit/slot/port | vlan id}

Режим Global Config

no arp

Данная команда удаляет запись ARP. Значение *arpentry* - это IP-адрес интерфейса. Значение **ipaddress** - это IP-адрес устройства в подсети, подключенной к существующему интерфейсу маршрутизации. Параметр **macaddr** является одноадресным MAC-адресом этого устройства. Параметр «**interface**» задает интерфейс следующего перехода.

Формат no arp *ipaddress* [interface {unit/slot/port | vlan vlan}]

Режим Global Config

arp cachesize

Данная команда позволяет настроить размер кэша ARP. Размер кэша ARP - это целое число, специфическое для своей платформы. Размер по умолчанию, соответственно, также отличается от платформы к платформе.

Формат arp cachesize platform specific integer value

Режим Global Config

no arp cachesize

Данная команда позволяет сбросить размер кэша ARP на значения по умолчанию.

Формат no arp cachesize

Режим Global Config

arp dynamicrenew

Данная команда позволяет компоненту ARP автоматически обновлять динамические записи ARP после их устаревания. Когда запись ARP достигает максимального возраста, система должна решить: сохранить или удалить запись. Если запись была недавно использована для пересылки пакетов данных, система обновит запись, отправив ARP-запрос соседнему устройству. Если соседнее устройство отвечает - возраст записи кэша ARP сбрасывается на 0 без удаления записи. Трафик на хост продолжает пересылаться без перерыва. Если запись не используется для пересылки пакетов данных, запись удаляется из кэша ARP, если только параметр динамического обновления не включен. Если же опция динамического обновления включена, система отправляет запрос ARP для обновления записи. Если запись не обновляется, она удаляется из устройства и последующие пакеты данных заставляют осуществить ARP-запрос. Трафик на хост может быть потерян до тех пор, пока маршрутизатор не получит ответ на ARP-запрос от хоста. Записи шлюза и записи для соседнего маршрутизатора обновляются всегда. Опция динамического обновления применяется только к записям хоста.

Недостатком динамического обновления является то, что после создания записи в кэше ARP эта запись продолжает занимать место в кэше до тех пор, пока сосед продолжает отвечать на запросы ARP, даже если трафик на него не перенаправляется. В сети, где количество потенциальных соседей больше, чем емкость кэша ARP, возможность динамического обновления может помешать некоторым соседям осуществлять коммуникацию из-за переполнения кеша ARP.

По умолчанию отключено

Формат arp dynamicrenew

Режим Privileged EXEC

no arp dynamicrenew

Данная команда отключает функцию обновления ARP-записей после их устаревания.

Формат no arp dynamicrenew

Режим Privileged EXEC

arp purge

Данная команда удаляет указанный IP-адрес из кэша ARP. Эта команда работает только с адресами типов «dynamic» и «gateway».

Формат arp purge *ipaddress* interface {*unit/slot/port* | vlan *id*}

Режим Privileged EXEC

Параметр	Описание
ipaddress	IP-адрес, который должен быть удален из кэша ARP.
interface	Интерфейс, из которого должны быть удалены IP-адреса.

arp resptime

Данная команда позволяет настроить таймаут ответа на ARP-запрос.

Значение **seconds** является действительным положительным целым числом, которое представляет собой время ответа на IP ARP-запись (в секундах). Значение **seconds** находится в пределах 1-10 секунд.

По умолчанию 1

Формат arp resptime 1-10

Режим Global Config

no arp resptime

Данная команда сбрасывает таймаут ответа на ARP-запрос к значениям по умолчанию.

Формат no arp resptime

Режим Global Config

arp retries

Данная команда позволяет настроить максимальное количество попыток для ARP-запроса.

Значение *retries* - целое число, представляющее собой максимально разрешенное количество повторных попыток. Значение *retries* находится в пределах 0-10 попыток.

По умолчанию 4

Формат arp retries 0-10

Режим Global Config

no arp retries

Данная команда сбрасывает максимальное количество попыток для ARP-запроса на значения по умолчанию.

Формат no arp retries

Режим Global Config

arp timeout

Данная команда позволяет настроить время устаревания записи ARP.

Значение **seconds** является действительным положительным целым числом, которое представляет собой время устаревания ARP-записи (в секундах). Значение **seconds** находится в пределах 15-21600 секунд.

По умолчанию 1200

Формат arp timeout *15-21600*

Режим Global Config

no arp timeout

Данная команда сбрасывает время устаревания записи ARP на значения по умолчанию.

Формат no arp timeout

Режим Global Config

clear arp-cache

Данная команда удаляет из кэша ARP все динамические ARP-записи. При указании ключевого слова «gateway» удаляются также динамические записи типа «gateway».

Формат clear arp-cache [gateway]

Режим Privileged EXEC

clear arp-switch

Данная команда удаляет содержимое таблицы ARP, содержащей записи, полученные через порт управления. Для того чтобы убедиться в том, что команда сработала, отправьте ping из удаленной системы на тестируемый коммутатор. Выполните команду **show arp switch**, чтобы увидеть записи ARP. Затем выполните команду **clear arp-switch** и проверьте записи, показываемые командой **arp switch**. Записей ARP быть не должно.

Фортма clear arp-switch

Режим Privileged EXEC

show arp

Данная команда показывает содержимое кэша ARP. Команда показывает не все записи ARP. Чтобы ознакомится со всеми записями ARP, используйте вывод команд show arp и show arp switch.

Формат show arp

Режим Privileged EXEC

Термин	Значение
Age Time (seconds)	Время устаревания записи ARP. Это значение настраивается. Измеряется в секундах.

Термин	Значение
Response Time (seconds)	Время таймаута запроса ARP. Это значение настраивается. Измеряется в секундах.
Retries	Максимальное количество повторных запросов ARP. Это значение настраивается.
Cache Size	Максимальное количество записей в таблице ARP. Это значение настраивается.
Dynamic Renew Mode	Предпринимает ли компонент ARP попытку обновить динамическую запись ARP после ее устаревания.
Total Entry Count Current / Peak	Общее и пиковое количество записей в таблице ARP.
Static Entry Count Current / Max	Общее и максимальное количество статических записей в таблице ARP.

Следующие параметры отображаются для каждой ARP-записи.

Термин	Значение
IP Address	IP-адрес устройства в подсети, подключенной к существующему интерфейсу маршрутизации.
MAC Address	Аппаратный MAC-адрес устройства.
Interface	Интерфейс, связанный с ARP-записью устройства.
Type	Один из настраиваемых типов. Возможные значения: Local, Gateway, Dynamic и Static.
Age	Текущий возраст записи ARP, с момента последнего обновления (в формате чч:мм:сс)

show arp brief

Данная команда показывает краткую информацию о таблице ARP.

Формат show arp brief

Режим Privileged EXEC

Термин	Значение
Age Time (seconds)	Время устаревания записи ARP. Это значение настраивается. Измеряется в секундах
Response Time (seconds)	Время таймаута запроса ARP. Это значение настраивается. Измеряется в секундах
Retries	Максимальное количество повторных запросов ARP. Это значение настраивается.
Cache Size	Максимальное количество записей в таблице ARP. Это значение настраивается.
Dynamic Renew Mode	Предпринимает ли компонент ARP попытку обновить динамическую запись ARP после ее устаревания.
Total Entry Count Current / Peak	Общее и пиковое количество записей в таблице ARP.
Static Entry Count Current / Max	Общее и максимальное количество статических записей в таблице ARP.

show arp switch

Эта команда отображает содержимое ARP-таблицы коммутатора.

Формат show arp switch

Режим Privileged EXEC

Термин	Значение
IP Address	IP-адрес устройства в подсети, подключенной к коммутатору.
MAC Address	Аппаратный MAC-адрес устройства.
Interface	Интерфейс, связанный с ARP-записью устройства.

8.2. Команды IP-маршрутизации

В этом разделе описаны команды, который используется для настройки функций IP-маршрутизации коммутатора.

routing

Данная команда включает маршрутизацию IPv4 и IPv6 на интерфейсе либо на группе интерфейсов. Текущее состояние этой функции можно вывести командой show ip brief. Значение обозначается как “Routing Mode”.

По умолчанию отключено

Формат routing

Режим Interface Config

no routing

Данная команда отключает маршрутизацию на интерфейсе.

Текущее состояние этой функции можно вывести командой show ip brief. Значение обозначается как “**Routing Mode**”.

Формат no routing

Режим Interface Config

ip routing

Данная команда активирует режим IP Router для Master-коммутатора.

Формат ip routing

Режим Global Config

no ip routing

Данная команда отключает режим IP Router для Master-коммутатора.

Формат no ip routing

Режим Global Config

ip address

Данная команда настраивает IP-адрес на интерфейсе или диапазоне интерфейсов. Вы можете использовать эту команду для настройки одного IP-адреса на интерфейсе. Команда поддерживает RFC 3021 и использование 31-битного префикса на IPv4 соединениях «точка-точка». Эта команда добавляет метку «IP address» для команды “show ip interface

”.

ПРИМЕЧАНИЕ: 31-битная маска подсети поддерживается только интерфейсами маршрутизации. Функция недоступна для сетевых и сервисных портов, потому что на этих управляющих интерфейсах коммутатор функционирует в качестве хоста, а не маршрутизатора.

Формат ip address ipaddr {subnetmask | /masklen}

Режим Interface Config

Параметр	Описание
ipaddr	IP-адрес интерфейса.
subnetmask	Маска подсети интерфейса.
masklen	Применение RFC 3021. При использовании «/»-нотации маски подсети, данное число указывает длину маски подсети. Диапазон - от 5 до 32 байт.

ПРИМЕР: В следующем Примере показана конфигурация маски подсети и IP-адреса, в десятичном формате, на интерфейсе 0/4/1.

```
(router1) #config
(router1) (Config)#interface 0/4/1
(router1) (Interface 0/4/1)#ip address 192.168.10.1 255.255.255.254
```

ПРИМЕР: В следующем Примере показана конфигурация маски подсети и IP-адреса, в «/»-нотации, на интерфейсе 0/4/1.

```
(router1) #config
(router1) (Config)#interface 0/4/1
(router1) (Interface 0/4/1)#ip address 192.168.10.1 /31
```

no ip address

Данная команда удаляет IP-адреса на интерфейсе. Параметр **ipaddr** – это IP-адрес интерфейса, в формате «a.b.c.d», где a, b, c и d – числа в диапазоне 1 - 255. Параметр **subnetmask** – это маска подсети интерфейса, в формате «a.b.c.d», где a, b, c и d – числа в диапазоне 1 - 255. Для удаления всех IP-адресов (основных), настроенных на интерфейсе, введите команду без параметров.

Формат no ip address [{*ipaddr subnetmask*}]

Режим Interface Config

ip address dhcp

Данная команда позволяет клиенту DHCPv4 работать с внутриполосным интерфейсом, чтобы он мог получать сетевую информацию (такую как IP-адрес, маску подсети и шлюз по умолчанию) с сетевого DHCP-сервера. Когда на интерфейсе включается DHCP, система автоматически удаляет все вручную настроенные адреса IPv4 на интерфейсе.

Для включения клиента DHCPv4 на внутриполосном интерфейсе и отправке DHCP сообщений с идентификатором клиента, используйте команду **ip address dhcp client-id** в режиме Interface Config.

По умолчанию отключено

Формат ip address dhcp [client-id]

Режим Interface Config

ПРИМЕР: В следующем Примере DHCPv4 включается на интерфейсе 0/4/1.

```
(router1) #config
```

```
(router1) (Config)#interface 0/4/1
(router1) (Interface 0/4/1)#ip address dhcp
```

no ip address dhcp

Данная команда освобождает арендуемый адрес и отключает DHCPv4 на интерфейсе. «**no**»-форма команды **ip address dhcp client-id** удаляет опцию «client-id» и отключает DHCP-клиент на внутриполосном интерфейсе.

Формат no ip address dhcp [client-id]

Режим Interface Config

ip default-gateway

Данная команда позволяет вручную настроить шлюз коммутатора по умолчанию. Можно настроить только один шлюз по умолчанию. Если вы выполните команду несколько раз, каждое новое значение будет заменять предыдущее.

Шлюз по умолчанию используется во всех случаях, когда у системы нет более точного пути для отправки пакета. Система устанавливает маршрут по умолчанию IPv4 с адресом шлюза в качестве адреса следующего перехода. Приоритет маршрута – 253. Шлюз по умолчанию, настроенный при помощи этой команды, имеет больший приоритет, чем шлюз, полученный от DHCP-сервера.

Формат ip default-gateway *ipaddr*

Режим Global Config

Параметр	Описание
ipaddr	IPv4-адрес подключенного маршрутизатора.

ПРИМЕР: Следующий пример демонстрирует настройку адреса шлюза по умолчанию на 10.1.1.1.

```
(router1) #config
(router1) (Config)#ip default-gateway 10.1.1.1
```

no ip default-gateway

Данная команда удаляет шлюз по умолчанию из конфигурации.

Формат no ip default-gateway *ipaddr*

Режим Interface Config

ip route

Данная команда позволяет настроить статический маршрут. Параметр *ipaddr* – действительный IP-адрес, параметр **subnetmask** – действительная маска подсети. Параметр **nexthopip** – действительный IP-адрес маршрутизатора следующего перехода. Необязательный параметр **preference** – целое число (от 1 до 255), позволяющее указать приоритет для данного статического маршрута. Среди маршрутов к одному и тому же месту назначения в базу данных пересылки вводится маршрут с наименьшим значением приоритета. Указав приоритет статического маршрута, вы определяете, является ли он

более или менее предпочтительным по сравнению с маршрутами динамических протоколов маршрутизации. Также приоритет определяет предпочтительность одних статических маршрутов перед другими. Маршрут с приоритетом 255 для пересылки трафика не используется.

Параметр «**description**» позволяет указать описание маршрута.

Для того, чтобы статические маршруты стали видимыми, необходимо выполнить следующие шаги:

- Глобально включить IP-маршрутизацию.
- Включить IP-маршрутизацию для интерфейса.
- Подтвердить, что связанный линк находится в состоянии «Up».

По умолчанию preference—1

Формат ip route ipaddr subnetmask { nexthopip | interface {unit/slot/port| vlanid}} [preference] [description description]

Режим Global Config

no ip route

Данная команда удаляет один статический маршрут. Параметр *nexthopip* позволяет удалить следующий переход. Параметр *preference* также сбрасывает приоритет статического маршрута на значение по умолчанию.

Формат no ip route ipaddr subnetmask [{nexthopip [preference]}]

Режим Global Config

ip route default

Данная команда позволяет настроить маршрут по умолчанию. Параметр *nexthopip* – действительный IP-адрес маршрутизатора следующего перехода. Параметр приоритета *preference* – десятичное число в диапазоне 1 – 255. Маршрут с приоритетом 255 для пересылки трафика не используется.

По умолчанию Preference— 1

Формат ip route default *nexthopip [preference]*

Режим Global Config

no ip route default

Данная команда удаляет все настроенные маршруты по умолчанию. Если указан необязательный параметр **nexthopip**, то следующий переход удаляется из настроенного маршрута по умолчанию. Если указан необязательный параметр «preference», приоритет маршрута будет сброшен на значения по умолчанию.

Формат no ip route default [{nexthopip | preference}]

Режим Global Config

ip route distance

Данная команда позволяет настроить длину (приоритет) для статических маршрутов. Меньшая длина маршрута имеет приоритет при вычислении лучшего маршрута. Команды

ip route и ip route default позволяют в случае необходимости настроить длину (приоритет) индивидуально для каждого статического маршрута. Если длина маршрута не указана, используется значение по умолчанию. Изменение длины по умолчанию не затрагивает изменение значения длины у тех маршрутов, которые были настроены ранее с предыдущим значением длины по умолчанию. Соответственно, новая длина по умолчанию будет применяться только к новым маршрутам.

По умолчанию 1

Формат ip route distance 1-255

Режим Global Config

no ip route distance

Данная команда устанавливает заводские значения для длины маршрута по умолчанию. Меньшая длина имеет приоритет при вычислении лучшего маршрута.

Формат no ip route distance

Режим Global Config

ip netdirbcast

Эта команда активирует пересылку направленных широковещательных передач на интерфейсе или в диапазоне интерфейсов. При включении направленные широковещательные передачи пересылаются. При отключении - отбрасываются.

По умолчанию отключено

Формат ip netdirbcast

Режим Interface Config

no ip netdirbcast

Эта команда отключает пересылку направленных широковещательных передач. При отключении широковещательные передачи не пересылаются.

Формат no ip netdirbcast

Режим Interface Config

ip mtu

Данная команда позволяет настроить IP MTU (Maximum Transmission Unit) для интерфейсу маршрутизации или диапазона интерфейсов. IP MTU - это максимальный размер пакета IP, который может быть передан на интерфейс без фрагментации. Пересылаемые пакеты отбрасываются, если их размер превышает значение IP MTU исходящего интерфейса.

Пакеты, созданные на маршрутизаторе, могут быть фрагментированы стеком IP.

ПРИМЕЧАНИЕ: Значение IP MTU является максимальным размером всего IP-пакета (IP-заголовок + полезные данные). Он не содержит дополнительных байтов, которые могут потребоваться для заголовков уровня 2. Для приема и обработки пакетов, Ethernet MTU (см. «Mtu» на стр. 343) должен учитывать размер заголовка Ethernet.

По умолчанию 1500 байт

Формат ip mtu *68-9198*

Режим Interface Config

no ip mtu

Данная команда возвращает значение IP MTU к настройкам по умолчанию.

Формат no ip mtu

Режим Interface Config

release dhcp

Данная команда заставляет клиента DHCPv4 освободить выданный адрес. DHCP-клиент отправляет сообщение DHCP Release, сообщающее DHCP-серверу, что данный IP-адрес более не нужен и может быть назначен другому клиенту.

Формат release dhcp {*unit/slot/port* | vlan *id*}

Режим Privileged EXEC

renew dhcp

Данная команда заставляет клиента DHCPv4 немедленно обновить адрес IPv4, выданный на указанном интерфейсе.

ПРИМЕЧАНИЕ: Данная команда может использоваться как на внутриполосных, так и внешних портах.

Формат renew dhcp {*unit/slot/port* | vlan *id*}

Режим Privileged EXEC

renew dhcp network-port

Данния команда обновляет IP-адрес на сетевом порте.

Формат renew dhcp network-port

Режим Privileged EXEC

encapsulation

Данная команда позволяет настроить тип инкапсуляции пакетов канального уровня OSI на интерфейсе либо на диапазоне интерфейсов. Возможные типы инкапсуляции: ethernet или snap.

По умолчанию ethernet

Формат encapsulation {ethernet | snap}

Режим Interface Config

ПРИМЕЧАНИЕ: При маршрутизации фреймов во VLAN всегда используется инкапсуляция ethernet.

show ip brief

Данная команда выводит сводную информацию о глобальной конфигурации IP, включая настройки ограничения ICMP и глобальные настройки ICMP Redirect.

Формат show ip brief

Режимы Privileged EXEC

User EXEC

Термин	Значение
Default Time to Live	Вычисленное значение TTL (Time to Live) пакета, пересылаемого локальным маршрутизатором на адрес назначения.
Routing Mode	Показывает, включен ли режим маршрутизации.
Maximum Next Hops	Максимальное количество переходов, которые может совершить пакет.
Maximum Routes	Максимальное количество маршрутов, которое может пройти пакет.
ICMP Rate Limit Interval	Показывает частоту инициализации буфера маркеров с токенами размера первышения. Интервал первышения: 0 – 2147483647 миллисекунд. Интервал первышения по умолчанию: 1000 миллисекунд.
ICMP Rate Limit Burst Size	Количество ICMPv4-сообщений об ошибке, которые могут отправлены за один интервал первышения. Диапазон: 1 – 200 сообщений. Значение по умолчанию: 100 сообщений.
ICMP Echo Replies	Включена ли функция ответа на эхо-запросы.
ICMP Redirects	Включена ли функция ICMP Redirects.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Switch) #show ip brief
Default Time to Live.....64
Routing Mode .....Disabled
Maximum Next Hops.....4
Maximum Routes.....128
ICMP Rate Limit Interval.....1000 msec
ICMP Rate Limit Burst Size .....100 messages
ICMP Echo Replies.....Enabled
ICMP Redirects.....Enabled
```

show ip interface

Данная команда отображает всю соответствующую информацию об интерфейсе IP. Аргумент «unit/slot/port» соответствует физическому интерфейсу маршрутизации либо интерфейсу маршрутизации VLAN. Ключевое слово vlan используется для указания VLAN ID, маршрутизируемой VLAN напрямую, вместо формата «unit/slot/port».

Формат show ip interface {unit/slot/port|vlan 1-4094}

Режимы Privileged EXEC

User EXEC

Термин	Значение
Routing Interface Status	Рабочее состояние интерфейса маршрутизации IPv4. Возможные значения: Up (работает) и Down (не работает).
Primary IP Address	Основной IP-адрес и маска подсети интерфейса. Значение отображается только в том случае, если оно было настроено ранее.
Method	Показывает способ распределения IP-адресов: вручную или с помощью сервера DHCP.
Routing Mode	Административный режим участия интерфейса в маршрутизации. Возможные значения: Enable (Включено) и Disable (Отключено). Это значение настраивается.
Administrative Mode	Административный режим указанного интерфейса. Возможные значения: Enable (Включено) и Disable (Отключено). Это значение настраивается.
Forward Net Directed Broadcasts	Включена или отключена передача направленных широковещательных пакетов. Это значение настраивается.
Active State	Информация о том, активен ли данный интерфейс или нет. Интерфейс считается активным, если его линк активен и он сам находится в состоянии пересылки.
Link Speed Data Rate	Скорость передачи данных указанного интерфейса. Измеряется в мегабитах в секунду (Мбит/с).
MAC Address	Физический адрес выбранного интерфейса. Формат - 6 двухзначных шестнадцатеричных чисел, разделенных двоеточиями.
Encapsulation Type	Тип инкапсуляции указанного интерфейса. Возможные типы: Ethernet либо SNAP.
IP MTU	Размер MTU фрейма, в байтах.

Термин	Значение
Bandwidth	Показывает пропускную способность интерфейса.
Destination Unreachables	Могут ли быть отправлены сообщения ICMP Destination Unreachable.
Термин	Значение
ICMP Redirects	Могут ли быть отправлены ICMP Redirect.
DHCP Client Identifier	Идентификатор клиента отображается только в том случае, если протокол DHCP включен с опцией client-id на внутриполосном интерфейсе. См. "ip address dhcp".

ПРИМЕР: Вывод командной строки для данной команды.

```
(switch)#show ip interface 1/0/2
Routing Interface Status..... Down
Primary IP Address ..... 1.2.3.4/255.255.255.0
Method ..... Manual
Helper IP Address..... 1.2.3.4
 ..... 1.2.3.5
Routing Mode ..... Disable
Administrative Mode ..... Enable
Forward Net Directed Broadcasts..... Disable
Active State..... Inactive
Link Speed Data Rate ..... Inactive
MAC Address..... 00:10:18:82:0C:68
Encapsulation Type..... Ethernet
IP MTU ..... 1500
Bandwidth..... 100000 kbps
Destination Unreachables..... Enabled
ICMP Redirects..... Enabled
```

ПРИМЕР: В приведенном Примере DHCP клиент включен на маршрутизироемом интерфейсе VLAN.

```
(Routing) #show ip interface vlan 10
Routing Interface Status..... Up
Method ..... DHCP
Routing Mode ..... Enable
Administrative Mode ..... Enable
Forward Net Directed Broadcasts..... Disable
```

Active State..... Inactive
Link Speed Data Rate ..... 10 Half
MAC address 00:10:18:82:16:0E
Encapsulation Type..... Ethernet
IP MTU 1500
Bandwidth..... 10000 kbps
Destination Unreachables..... Enabled
ICMP Redirects..... Enabled
Interface Suppress Status..... Unsuppressed
DHCP Client Identifier..... 0fastpath-0010.1882.160E-vl10

show ip interface brief

Данная команда отображает сводную информацию об IP-конфигурации всех портов маршрутизатора, и указывает, каким образом был назначен каждый IP-адрес.

Формат show ip interface brief

Режим Privileged EXEC
User EXEC

Термин	Значение
Interface	Корректные номера слота и порта разделяются косой чертой.
State	Рабочее состояние функции маршрутизации на интерфейсе.
IP Address	IP-адрес интерфейса маршрутизации, в 32-битном десятичном формате.
IP Mask	IP-маска интерфейса маршрутизации, в 32-битном десятичном формате.
Method	Указывает, каким образом был назначен каждый IP-адрес. Поле содержит одно из следующих значений: • DHCP - Адрес был назначен DHCP-сервером. • Manual - Адрес был назначен вручную.

ПРИМЕР: Вывод командной строки для данной команды.

```
(alpha1) #show ip interface brief
Interface        State      IP Address      IP Mask         Method
-------------------------------------------------------------------------
1/0/17           Up         192.168.75.1    255.255.255.0   DHCP
```

show ip route

Данная команда отображает таблицу маршрутизации. Параметр *ip-address* отображает сеть, для которой должен отображаться маршрут, а также отображает наилучший оптимальный маршрута для адреса. Параметр **mask** – маска подсети указанного IP-адреса **ip-address**. При использовании ключевого слова **longer-prefixes**, пара **ip-address** и **mask** становится префиксом, и команда отображает маршруты к адресам, совпадающим с данным префиксом. Параметр **protocol** указывает протокол, устанавливающий маршруты. Возможные значения **protocol**: **connected** либо **static**. Использование параметра **all** выводи все маршруты, оптимальные и неоптимальные. Без параметра **all** команда будет отображать только лучшие маршруты.

ПРИМЕЧАНИЕ: При использовании значения **connected** для **protocol** параметр **all** недоступен, потому что в таком случае нет оптимального и неоптимального маршрута.

ПРИМЕЧАНИЕ: При использовании ключевого слова static для параметра **protocol** также доступна опция **description**, например **show ip route ip-address static description**. Данная команда отображает описания статических маршрутов.

Формат show ip route [{ip-address [protocol] | {ip-address mask [longer-prefixes] [protocol] | protocol} [all] | all}]

Режимы Privileged EXEC

User EXEC

Термин	Значение
Route Codes	Ключевые слова для кодов протокола маршрутизации, которые могут появиться в выводе таблицы.

Команда show ip route отображает таблицы маршрутизации в одном из следующих форматов:

Code IP-Address/Mask [Preference/Metric] via Next-Hop, Route-Timestamp, Interface, Truncated

Столбцы для таблицы маршрутизации отображают следующую информацию:

Термин	Значение
Code	Коды протоколов маршрутизации, создающих маршруты.
Default Gateway	IP-адрес шлюза по умолчанию. Шлюз по умолчанию используется во всех случаях, когда у системы нет более точного пути для отправки пакета
IP-Address/Mask	IP-адрес и маска сети назначения, соответствующие маршруту.
Preference	Административный приоритет маршрута. Маршруты с низким значением имеют приоритет перед маршрутами с высоким.
Metric	«Стоимость» маршрута.

Термин	Значение
via Next-Hop	Внешний IP-адрес маршрутизатора, используемый при пересылке трафика на следующий маршрутизатор (если есть) на пути к месту назначения.
Route-Timestamp	Время последнего обновления динамических маршрутов. Формат: Дней:Часов:Минут, если количество дней не меньше одного Часов:Минут:Секунд, если количество дней меньше одного
Interface	Исходящий интерфейс маршрутизатора, используемый при пересылке трафика к следующему пункту назначения.
T	Флаг, добавленный к маршруту, чтобы указать, что это маршрут ECMP, но только один из его следующих переходов был добавлен в таблицу пересылки. Таблица пересылки может ограничивать количество маршрутов или групп ECMP. Когда маршрут ECMP не может быть установлен по причине достижения такого предела, маршрут устанавливается с одним последующим переходом. Такие усеченные маршруты идентифицируются меткой T после имени интерфейса.

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show ip route
Route Codes: C - Connected, S - Static
Default gateway is 1.1.1.2
C 1.1.1.0/24 [0/1] directly connected, 0/11
C 2.2.2.0/24 [0/1] directly connected, 0/1
C 5.5.5.0/24 [0/1] directly connected, 0/5
S 7.0.0.0/8 [1/0] directly connected, Null0
OIA 10.10.10.0/24 [110/6] via 5.5.5.2,  00h:00m:01s,  0/5

C 11.11.11.0/24 [0/1] directly connected,  0/11
S 12.0.0.0/8 [5/0] directly connected, Null0
S 23.0.0.0/8 [3/0] directly connected, Null0
C 1.1.1.0/24 [0/1] directly connected, 0/11
C 2.2.2.0/24 [0/1] directly connected, 0/1
C 5.5.5.0/24 [0/1] directly connected, 0/5
C 11.11.11.0/24 [0/1] directly connected, 0/11
S 10.3.2.0/24 [1/0] via 1.1.1.2, 0/11
```

ПРИМЕР: Выполнение команды, вывод отображает усеченные маршруты.

```
(router) #show ip route
Route Codes:  C - Connected, S - Static
O E1   100.1.161.0/24 [110/10] via 172.20.11.100,   00h:00m:13s,  2/11 T
O E1   100.1.162.0/24 [110/10] via 172.20.11.100,   00h:00m:13s,  2/11 T
O E1   100.1.163.0/24 [110/10] via 172.20.11.100,   00h:00m:13s,  2/11 T
```

show ip route ecmp-groups

Эта команда выводит все текущие ECMP-группы в таблице маршрутизации IPv4. Группа ECMP представляет собой набор из двух или более следующих переходов, используемых в одном или нескольких маршрутах. Группы нумеруются произвольно от 1 до n. Вывод указывает количество следующих переходов в группе и количество маршрутов, которые используют данный набор переходов. Вывод команды показывает IPv4-адреса и исходящие интерфейсы каждого следующего перехода в каждой группе.

Формат show ip route ecmp-groups

Режим Privileged EXEC

ПРИМЕР: Пример вывода командной строки для данной команды.

```
(router) #show ip route ecmp-groups
ECMP Group 1 with 2 next hops (used by 1 route)
  172.20.33.100 on interface 2/33
  172.20.34.100 on interface 2/34
ECMP Group 2 with 3 next hops (used by 1 route)
  172.20.32.100 on interface 2/32
  172.20.33.100 on interface 2/33
  172.20.34.100 on interface 2/34
ECMP Group 3 with 4 next hops (used by 1 route)
  172.20.31.100 on interface 2/31
  172.20.32.100 on interface 2/32
  172.20.33.100 on interface 2/33
  172.20.34.100 on interface 2/34
```

show ip route summary

Данная команда отображает сводную информацию о состояни таблицы маршрутизации. Необязательное ключевое слово all показывает некоторые статистические параметры (такие как количество маршрутов из каждого источника, в том числе альтернативных маршрутов). Альтернативный маршрут - это маршрут, который не является наиболее предпочтительным маршрутом к месту назначения и поэтому не сохранен в таблице переадресации. Чтобы включить только информацию об оптимальных маршрутах, не используйте ключевые слова.

Формат show ip route summary [all]

Режимы Privileged EXEC

User EXEC

Термин	Значение
Connected Routes	Общее количество подключенных маршрутов в таблице маршрутизации.
Static Routes	Общее количество статических маршрутов в таблице маршрутизации.
Total Routes	Общее количество маршрутов в таблице маршрутизации.
Best Routes (High)	Общее количество оптимальных маршрутов в таблице маршрутизации на данный момент. Учитываются только оптимальные маршуты к каждому месту назначения. Значения в скобках указывает максимальное количество уникальных оптимальных маршрутов с момента последней очистки статистики.
Alternate Routes	Общее количество альтернативных маршрутов, присутствующих в таблице маршрутизации. Альтернативный маршрут - это маршрут, который не является оптимальным маршрутом к месту назначения.
Route Adds	Количество маршрутов, добавленных в таблицу маршрутизации.
Route Modifies	Число маршрутов, которые были изменены после того, как они были добавлены в таблицу маршрутизации.
Route Deletes	Количество маршрутов, удаленных из таблицы маршрутизации.
Unresolved Route Adds	Количество добавленных маршрутов, которые не смогли быть использованы по причине того что ни один из следующих переходов маршрута не был в локальной подсети. Обратите внимание, что статические маршруты не могут быть добавлены в таблицу маршрутизации при загрузке, потому что интерфейсы маршрутизации еще не установлены. В этом случае счетчик увеличивается на 1. Статические маршруты добавляются в таблицу маршрутизации при появлении интерфейсов маршрутизации.
Invalid Route Adds	Количество маршрутов, которые не удалось добавить в силу того, что маршрут был неверным. Для каждой из этих ошибок приводится сообщение журнала.
Failed Route Adds	Количество маршрутов, которые не удалось добавить в силу ограничения ресурсов таблицы маршрутизации.

Термин	Значение
Reserved Locals	Количество записей таблицы маршрутизации, зарезервированных для локальной подсети, на интерфейсе маршрутизации. Пространство для локальных маршрутов всегда резервируется таким образом, так что локальные маршруты могут быть установлены в случае сбоя работы интерфейса маршрутизации.
Unique Next Hops (High)	Количество уникальных последующих переходов, используемых среди всех маршрутов, находящихся в настоящее время в таблице маршрутизации. К ним относятся локальные интерфейсы для локальных маршрутов и соседей для непрямых маршрутов. Значения в скобках указывает максимальное количество уникальных переходов с момента последней очистки статистики.
Next Hop Groups (High)	Текущее количество групп последующих переходов, используемых в одном или несколько маршрутах. Каждая следующая группа переходов включает в себя один или несколько последующих переходов. Значения в скобках указывает максимальное количество групп последующих переходов с момента последней очистки статистики.
ECMP Groups (High)	Количество групп, содержащих несколько последующих переходов. Значения в скобках указывает максимальное количество групп последующих переходов с момента последней очистки статистики.
ECMP Groups	Количество групп, содержащих несколько последующих переходов.
ECMP Routes	Количество маршрутов с несколькими последующими переходами, находящимися в таблице маршрутизации в настоящий момент.
Truncated ECMP Routes	Количество маршрутов ECMP, установленных в настоящий момент в таблице пересылки, с единственным следующим переходом. Таблица пересылки может ограничивать количество маршрутов или групп ECMP. Когда маршрут ECMP не может быть установлен по причине достижения такого предела, маршрут устанавливается с одним последующим переходом.
ECMP Retries	Количество маршрутов ECMP, установленных в таблице пересылки, которые изначально были установлены только с одной точкой перехода.

Термин	Значение
Routes with n Next Hops	Текущее количество маршрутов, с количеством следующих переходов.

ПРИМЕР: Пример вывода командной строки для данной команды.

```
(Routing) #show ip route summary
Connected Routes ..... 7
Static Routes ..... 1
Total routes ..... 1032
Best Routes (High) ..... 1032 (1032)
Alternate Routes ..... 0
Route Adds ..... 1010
Route Modifies ..... 1
Route Deletes ..... 10
Unresolved Route Adds ..... 0
Invalid Route Adds ..... 0
Failed Route Adds ..... 0
Reserved Locals ..... 0
Unique Next Hops (High) ..... 13 (13)
Next Hop Groups (High) ..... 13 (14)
ECMP Groups (High) ..... 2 (3)
ECMP Routes ..... 1001
Truncated ECMP Routes ..... 0
ECMP Retries ..... 0
Routes with 1 Next Hop ..... 31
Routes with 2 Next Hops ..... 1
Routes with 4 Next Hops ..... 1000
```

clear ip route counters

Данная команда сбрасывает до нуля счетчики таблицы маршрутизации IPv4, отображаемые командой “show ip route summary”. Сбрасываются только счетчики событий. Те счетчики, которые содержат информацию о текущем состоянии таблицы маршрутизации (например, счетчик количества маршрутов каждого типа) не сбрасываются.

Формат clear ip route counters

Режим Privileged EXEC

show ip route preferences

Данная команда отображает подробную информацию о приоритетах (preferences) для каждого типа маршрута. Приоритеты используются для выявления оптимального маршрута. Более низкие значения приоритета являются предпочтительными перед более высокими. Маршрут с приоритетом 255 для пересылки трафика не используется.

Формат show ip route preferences

Режимы Privileged EXEC

User EXEC

Термин	Значение
Local	Значение приоритета локального маршрута.
Static	Значение приоритета статического маршрута.
Configured Default Gateway	Значение приоритета маршрута статически настроенного шлюза по умолчанию.
DHCP Default Gateway	Значение приоритета маршрута шлюза по умолчанию, полученного от сервера DHCP.

ПРИМЕР: Вывод командной строки для данной команды.

```
(alpha-stack) #show ip route preferences
Local.....0
Static.....1
Configured Default Gateway.....253
DHCP Default Gateway.....254
```

show ip stats

Даннная команда отображает статистическую информацию IP.

Формат show ip stats

Режимы Privileged EXEC

User EXEC

show routing heap summary

Данная команда отображает сводную информацию о распределения памяти из области, выделенной для маршрутизации. Область памяти для маршрутизации резервируется при загрузке системы, и используется только для приложений маршрутизации.

Формат show routing heap summary

Режим Privileged EXEC

Параметр	Описание
Heap Size	Объем памяти, в байтах, выделяемый при загрузке для области маршрутизации.
Memory In Use	Объем уже распределенной памяти, в байтах.
Memory on Free List	Объем свободной памяти из выделенной для маршрутизации области, в байтах. При освобождении некоторого объема памяти, она может использоваться повторно.
Memory Available in Heap	Количество байт в выделенной области памяти, которые никогда не использовались.
In Use High Water Mark	Максимальный показатель использования памяти с момента последней загрузки.

ПРИМЕР: Привет вывода командной строки для данной команды.

```
(Router) #show routing heap summary
Heap Size.....95053184
Memory In Use.....56998
Memory on Free List.....47
Memory Available in Heap.....94996170
In Use High Water Mark.....57045
```

8.3. Команды политики маршрутизации

show ip policy

Данная команда отображает карту маршрутов, связанную с каждым интерфейсом.

Формат show ip policy

Режим Privileged EXEC

Термин	Значение
Interface	Интерфейс.
Route-map	Карта маршрута

8.4. Команды RDP

В этом разделе описаны команды, который используется для настройки протокола RDP (Router Discovery Protocol). Протокол RDP позволяет хосту обнаруживать IP-адрес маршрутизаторов в подсети.

ip irdp

Эта команда активирует функцию обнаружения маршрутизатора на интерфейсе или в диапазоне интерфейсов.

По умолчанию отключено

Формат ip irdp

Режим Interface Config

no ip irdp

Данная команда отключает функцию обнаружения маршрутизатора на интерфейсе.

Формат no ip irdp

Режим Interface Config

ip irdp address

Эта команда настраивает адрес, который используется интерфейсом для отправки объявлений обнаружения маршрутизатора. Допустимое значение для *ipaddr*: 255.255.255.255 (ограниченный широковещательный адрес).

По умолчанию 224.0.0.1

Формат ip irdp address ipaddr

Режим Interface Config

no ip irdp address

Данная команда настраивает адрес по умолчанию, используемый для объявления маршрутизатора для интерфейса.

Формат no ip irdp address

Режим Interface Config

ip irdp holdtime

Эта команда настраивает значение (в секундах) для поля «holdtime» объявлений маршрутизатора, отправляемых с этого интерфейса. Диапазон составляет от 4 до 9000 секунд.

По умолчанию 3 * maxinterval

Формат ip irdp holdtime 4-9000

Режим Interface Config

no ip irdp holdtime

Эта команда устанавливает значение по умолчанию для поля «holdtime» объявлений маршрутизатора, отправляемых с этого интерфейса.

Формат no ip irdp holdtime

Режим Interface Config

ip irdp maxadvertinterval

Эта команда настраивает максимальное время (в секундах) между отправкой объявлений маршрутизатора с интерфейса. Диапазон - от 4 до 1800 секунд.

По умолчанию 600

Формат ip irdp maxadvertinterval 4-1800

Режим Interface Config

no ip irdp maxadvertinterval

Эта команда устанавливает значение по умолчанию для максимального времени (в секундах) между отправкой объявлений маршрутизатора с интерфейса.

Формат no ip irdp maxadvertinterval

Режим Interface Config

ip irdp minadvertinterval

Эта команда настраивает минимальное время (в секундах) между отправкой объявлений маршрутизатора с интерфейса. Диапазон - от 3 до 1800 секунд.

По умолчанию 0.75 * maxadvertinterval

Формат ip irdp minadvertinterval 3-1800

Режим Interface Config

no ip irdp minadvertinterval

Эта команда устанавливает значение по умолчанию для минимального времени (в секундах) между отправкой объявлений маршрутизатора с интерфейса.

Формат no ip irdp minadvertinterval

Режим Interface Config

ip irdp multicast

Эта команда настраивает для объявлений маршрутизатора IP-адрес назначения 224.0.0.1, который является адресом по умолчанию. «No»-форма настраивает IP-адрес 255.255.255.255, чтобы вместо этого отправлять объявления маршрутизатора на ограниченный широковещательный адрес.

Формат ip irdp multicast *ip address*

Режим Interface Config

no ip irdp multicast

По умолчанию объявления маршрутизатора отправляются на 224.0.0.1. Чтобвы настроить отправку объявлений маршрутизатора на ограниченный широковещательный адрес 255.255.255.255, используйте «No»-форму этой команды.

Формат no ip irdp multicast

Режим Interface Config

ip irdp preference

Эта команда настраивает приоритет для адреса маршрутизатора по умолчанию, по отношению к другим адресам маршрутизатора в той же подсети.

По умолчанию 0

Формат ip irdp preference -2147483648 to 2147483647

Режим Interface Config

no ip irdp preference

Эта команда устанавливает приоритет по умолчанию для адреса маршрутизатора, по отношению к другим адресам маршрутизатора в той же подсети.

Формат no ip irdp preference

Режим Interface Config

show ip irdp

Данная команда отображает информацию, относящуюся к RDP, для указанного интерфейса, всех интерфейсах или определенной VLAN. Аргумент «unit/slot/port» соответствует физическому интерфейсу маршрутизаци либо интерфейсу маршрутизации VLAN. Ключевое слово **vlan** используется для указания VLAN ID маршрутизирующей VLAN напрямую, вместо формата «unit/slot/port».

Формат show ip irdp {unit/slot/port|vlan 1-4094|all}

Режим Privileged EXEC

User EXEC

Термин	Значение
Interface	Аргумент «unit/slot/port» соответствует физическому интерфейсу маршрутизаци либо интерфейсу маршрутизаци vlan.
vlan	Ключевое слово vlan используется для указания VLAN ID маршрутизирующей VLAN напрямую, вместо формата «unit/slot/port».
Ad Mode	Включена или выключена на данном интерфейсе функция обнаружения маршрутизатора.
Dest Address	IP-адрес назначения для объявлений маршрутизатора.
Max Int	Максимальное время (в секундах) между отправкой объявлений маршрутизатора с интерфейса.
Min Int	Минимальное время (в секундах) между отправкой объявлений маршрутизатора с интерфейса.

Термин	Значение
Hold Time	Количество времени в секундах, в течение которого система должна хранить обявления маршрутизатора перед их удалением.
Preference	Приоритет для адреса маршрутизатора по умолчанию, по отношению к другим адресам маршрутизатора в той же подсети.

8.5. Команды маршрутизации VLAN

В этом разделе описаны команды, который используется для настройки маршрутизации VLAN и для просмотра информации о текущем состоянии маршрутизации VLAN.

vlan routing

Данная команда включает маршрутизацию в сети VLAN. Диапазон значений vlanid: 1 – 4094. Значение *[*interface ID*]* имеет диапазон от 1 до 64. Как правило, вводить ID интерфейса не требуется, так как система выбирает его самостоятельно в автоматическом режиме. Однако при указании ID интерфейса он становится номером порта в unit/slot/port для интерфейса маршрутизации VLAN. При выборе идентификатора уже используемого интерфейса система выведет сообщение об ошибке, интерфейс VLAN создан не будет.

Формат vlan routing vlanid [interface ID]

Режим VLAN Config

no vlan routing

Данная команда отключает маршрутизацию в сети VLAN.

Формат no vlan routing vlanid

Режим VLAN Config

ПРИМЕР: В примере 1 показано выполнение команды с указанием vlanid. Идентификатор интерфейса не указывается.

```
(Switch)(Vlan)#vlan 14
(Switch)(Vlan)#vlan routing 14 ?
<cr>          Press enter to execute the command.
<1-24>        Enter interface ID
```

Нажатие кнопки <Enter> без указания ID интерфейса, как правило, заставляет систему выбрать ID интерфейса автоматически.

ПРИМЕР: В примере 2 показано выполнение команды с указанием interface ID 51 для интерфейса VLAN 14. Идентификатор интерфейса становится номером порта в unit/slot/port для интерфейса маршрутизации VLAN. В данном Примере unit/slot/port принимает значение 4/51 для интерфейса VLAN 14.

```
(Switch)(Vlan)#vlan 14 51
```

```
(Switch)(Vlan)#
(Switch)#show ip vlan
MAC Address used by Routing VLANs:   00:11:88:59:47:36
```

VLAN ID	Logical Interface	IP Address	Subnet Mask
10	4/1	172.16.10.1	255.255.255.0
11	4/50	172.16.11.1	255.255.255.0
12	4/3	172.16.12.1	255.255.255.0
13	4/4	172.16.13.1	255.255.255.0
14	4/51	0.0.0.0	0.0.0.0

```
<--u/s/p is 4/51 for VLAN 14 interface
```

ПРИМЕР: В примере 3 показана попытка выбрать интерфейс, который уже используется. В этом случае интерфейс командной строки выдает сообщение об ошибке, интерфейс VLAN не создается.

```
(Switch) #show ip vlan
MAC Address used by Routing VLANs:   00:11:88:59:47:36
```

VLAN ID	Logical Interface	IP Address	Subnet Mask
10	4/1	172.16.10.1	255.255.255.0
11	4/50	172.16.11.1	255.255.255.0
12	4/3	172.16.12.1	255.255.255.0
13	4/4	172.16.13.1	255.255.255.0
14	4/51	0.0.0.0	0.0.0.0

```
(Switch)#config
(Switch)(Config)#exit
(Switch)#vlan database
(Switch)(Vlan)#vlan 15
(Switch)(Vlan)#vlan routing 15 1
Interface ID 1 is already assigned to another interface
```

interface vlan

Данная команда используется для входа в режим настройки интерфейса для указанной VLAN. Диапазон vlan-id – от 1 до 4094.

Формат interface vlan vlan-id

Режим Global Config

show ip vlan

Данная команда отображает информацию о маршрутизации VLAN для всех VLAN, на которых включена маршрутизация.

Формат show ip vlan

Режимы Privileged EXEC

User EXEC

Термин	Значение
MAC Address used by Routing VLANs	MAC-адрес, связанный с внутренним интерфейсом маршрутизции коммутатора. Этот MAC-адрес используется всеми интерфейсами маршрутизации VLAN. Он будет отображаться выше информации VLAN.
VLAN ID	Идентификатор VLAN.
Logical Interface	Логический *unit/slot/port* , связанный с интерфейсом маршрутизации VLAN.
IP Address	IP-адрес, связанный с данной VLAN.
Subnet Mask	Маска подсети, связанная с этой VLAN.

8.6. Команды DHCP и BOOTP Relay

В этом разделе описаны команды, который используется для настройки BootP/DHCP Relay на коммутаторе. Агент DHCP relay работает на уровне 3 OSI, пересылая запросы и ответы DHCP между клиентами и серверами, если они не находятся в одной физической подсети.

bootpdhcprelay cidoptmode

Данная команда включает режим «circuit ID option» для BootP/DHCP Relay.

По умолчанию отключено

Формат bootpdhcprelay cidoptmode

Режим Global Config

no bootpdhcprelay cidoptmode

Данная команда отключает режим «circuit ID option» для BootP/DHCP Relay.

Формат no bootpdhcprelay cidoptmode

Режим Global Config

bootpdhcprelay maxhopcount

Данная команда настраивает максимально разрешенное количество переходов для BootP/DHCP Relay. Диапазон значений: 1 – 16.

По умолчанию 4

Формат bootpdhcprelay maxhopcount 1-16

Режим Global Config

no bootpdhcprelay maxhopcount

Данная команда возвращает на значение по умолчанию максимально разрешенное количество переходов для BootP/DHCP Relay.

Формат no bootpdhcprelay maxhopcount

Режим Global Config

bootpdhcprelay minwaittime

Данная команда настраивает минимальное время ожидания (в секундах) для BootP/DHCP Relay. Когда агент BOOTP relay получает сообщение BOOTREQUEST, он МОЖЕТ использовать поле seconds-since-client-began-booting («количество секунд с начала процесса загрузки клиента») запроса в качестве фактора при принятии решения о том, передавать запрос или нет. Диапазон значений: 0 – 100.

По умолчанию 0

Формат bootpdhcprelay minwaittime 0-100

Режим Global Config

no bootpdhcprelay minwaittime

Данная команда возвращает на значение по умолчанию минимальное время ожидания (в секундах)) для BootP/DHCP Relay в системе.

Формат no bootpdhcprelay minwaittime

Режим Global Config

show bootpdhcprelay

Данная команда отображает информацию BootP/DHCP Relay.

Формат show bootpdhcprelay

Режимы Privileged EXEC

User EXEC

Термин	Значение
Maximum Hop Count	Максимально допустимое количество переходов relay-агента.
Minimum Wait Time (Seconds)	Минимальное время ожидания.
Admin Mode	Включена или выключена ретрансляция запросов.

Термин	Значение
Circuit Id Option Mode	Включена или выключена опция circuit Id DHCP.

show ip bootpdhcprelay

Данная команда отображает информацию BootP/DHCP Relay.

Формат show ip bootpdhcprelay

Режим User EXEC

Параметр	Значение
Maximum Hop Count	Максимально допустимое количество переходов relay-агента.
Minimum Wait Time (Seconds)	Минимальное время ожидания.
Admin Mode	Включена или выключена ретрансляция запросов.
Circuit Id Option Mode	Включен или выключена опция circuit Id DHCP.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) >show ip bootpdhcprelay
Maximum Hop Count.....4
Minimum Wait Time(Seconds).....0
Admin Mode.....Disable
Circuit Id Option Mode .....Enable
```

8.7. Команды IP Helper

В этом разделе описываются команды, используемые для настройки и мониторинга агента IP Helper. IP Helper ретранслирует пакеты DHCP и другие широковещательные UDP-пакеты от локального клиента к одному или нескольким серверам, которые не находятся в одной сети с клиентом.

Функция IP Helper обеспечивает механизм, который позволяет маршрутизатору пересылать определенные широковещательные пакеты UDP на определенный IP-адрес. Это позволяет различным приложениям достигать серверов за пределами локальных подсетей (даже если приложение рассчитывает на постоянное нахождение сервера в локальной подсети) и использует широковещательные пакеты для установления контакта с сервером.

Администратор может настраивать записи ретранслятора как глобально, так и на интерфейсе маршрутизации. Каждая запись ретранслятора сопоставляет входной интерфейс и номер UDP-порта назначения с одним адресом IPv4 (адресом Helper). Администратор может настраивать несколько записей ретранслятора для одного и того

же интерфейса и UDP-порта, и в этом случае агент ретранслирует связанные пакеты на адрес каждого сервера. Конфигурация интерфейса имеет приоритет над глобальной конфигурацией. То есть, если UDP-порт назначения пакета соответствует любой записи на входном интерфейсе, пакет обрабатывается в соответствии с конфигурацией интерфейса. Если пакет не соответствует ни одной записи на входном интерфейсе, пакет обрабатывается в соответствии с глобальной конфигурацией IP-helper.

Администратор также может настроить запрещающие записи ретрансляции, которые будут отклонять соответствующе пакеты. Запрещающие записи используются для отклонения тех пакетов, полученных на определенном интерфейсе, которые в противном случае были бы ретранслированы в соответствии с глобальной записью ретрансляции. Запрещающие записи могут быть настроены только на интерфейсе (не глобально).

Кроме адресов сервера, администратор также настраивает, какие именно порты UDP пересылаются. Некоторые UDP-порты для удобства могут быть указаны по их имени в пользовательском интерфейсе, но для настройки записи ретранслятора подходит любой номер порта UDP. Администратор также может настривать запись ретранслятора, не содержащую UDP-порт назначения. Агент ретранслятора пересылает пакеты, удовлетворяющие условиям таких записей с портами назначения UDP. Это список стандартных портов.

Wildcard	UDP Port Number
IEN-116 Name Service	42
DNS	53
NetBIOS Name Server	137
NetBIOS Datagram Server	138
TACACS Server	49
Time Service	37
DHCP	67
Trivial File Transfer Protocol (TFTP)	69

Система ограничивает количество записей ретранслятора на значении, в четыре раза превышающем максимальное количество интерфейсов маршрутизации. Сетевой администратор может распределять записи ретранслятора по своему усмотрению. Количество записей на одном интерфейсе не ограничено, также как и количество серверов для пары «интерфейс - UDP-порт».

Ретранслятор передает DHCP пакеты в обоих направлениях. Он ретранслирует широковещательные пакеты от клиента на один или несколько DHCP-серверов, и передает обратно одноадресные пакеты DHCP-сервера. Для других протоколов агент ретрансляции передает только широковещательные пакеты от клиента к серверу. Предполагается, что пакеты от сервера к клиенту будут одноадресными. Поскольку в

обратном направлении нет ретранслятора для протоколов, отличных от DHCP, агент ретранслятора сохраняет исходящий IP-адрес из исходного клиентского пакета. Агент ретранслятора использует локальный IP-адрес в качестве источника ретраслируемого клиентского пакета DHCP.

Когда коммутатор принимает широковещательный UDP-пакет на интерфейсе маршрутизации, агент ретранслятора проверяет, настроен ли интерфейс для передачи данных с UDP-портом назначения. Если это так, агент перенаправляет пакет на настроенные IP-адреса сервера. В противном случае агент проверяет, существует ли глобальная конфигурация для UDP-порта назначения. Если это так, агент ретрансляции перенаправляет пакет на настроенные IP-адреса сервера. В противном случае пакет не ретранслируется. Обратите внимание, что если пакет соответствует запрещающей записи ретранслятора на входном интерфейсе, то пакет не пересылается, независимо от глобальной конфигурации.

Агент ретранслятора пересылает пакет только при выполнении следуюших условий:

MAC-адрес назначения должен быть широковещательным адресом (FF: FF: FF: FF: FF: FF)

IP-адрес назначения должен быть ограниченным широковещательным адресом (255.255.255.255) или адресом направленной широковещательной передачи для принимающего интерфейса.

Значение IP TTL должно быть больше 1.

Поле протокола в заголовке IP должно быть UDP (17).

UDP-порт назначения должен совпадать с портом в записи ретранслятора.

clear ip helper statistics

Данная команда сбрасывает показатели статистики, отображаемые командой **ip helper statistics**.

Формат clear ip helper statistics

Режим Privileged EXEC

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(switch) #clear ip helper statistics
```

ip helper-address (Global Config)

Данная команда используется для настройки ретрансляции определенных широковещательных пакетов UDP, получаемых на любом интерфейсе. Эту команду можно вызвать несколько раз, чтобы указать несколько адресов сервера для данного номера порта UDP, или указать несколько номеров портов UDP, обрабатываемых определенным сервером.

По умолчанию Адреса не настроены.

Формат ip helper-address server-address [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]

Режим Global Config

Параметр	Описание
server-address	Однонаправленный или направленный широковещательный адрес IPv4, на который отправляются ретранслируемые пакеты UDP. Этот адрес не может совпадать с IP-адресом одного из интерфейсов локального маршрутизатора.
dest-udp-port	Номер UDP-порта назначения, от 0 до 65535.
port-name	Опционально порты UDP могут иметь свои имена. Порт может указываться как по имени, так и по номеру. Имена портов: • dhcp (порт 67) • domain (порт 53) • isakmp (порт 500) • mobile-ip (порт 434) • nameserver (порт 42) • netbios-dgm (порт 138) • netbios-ns (порт 137) • ntp (порт 123) • pim-auto-rp (порт 496) • rip (порт 520) • tacacs (порт 49) • tftp (порт 69) • time (порт 37) Остальные порты должны указываться по номеру.

ПРИМЕР: Для ретрансляции пакетов DHCP, полученных на любом интерфейсе, на два DHCP-сервера: 10.1.1.1 и 10.1.2.1 - используйте следующие команды:

```
(switch)#config
(switch)(config)#ip helper-address 10.1.1.1 dhcp
(switch)(config)#ip helper-address 10.1.2.1 dhcp
```

ПРИМЕР: Для ретрансляции пакетов UDP, полученных на любом интерфейсе для всех стандартных портов, на сервер 20.1.1.1, используйте следующие команды:

```
(switch)#config
(switch)(config)#ip helper-address 20.1.1.1
```

no ip helper-address (Global Config)

Данная команда удаляет запись IP helper. Команда no ip helper-address без дополнительных аргументов удаляет все глобальные адреса IP helper.

Формат no ip helper-address [server-address [dest-udp-port | dhcp | domain | isakmp | mobileip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]

Режим Global Config

ip helper-address (Interface Config)

Данная команда используется для настройки ретрансляции определенных широковещательных пакетов UDP, полученных на определенном интерфейсе или диапазоне интерфейсов. Эту команду можно вызвать на интерфейсе маршрутизации несколько раз, чтобы указать несколько адресов сервера для данного номера порта, или указать несколько номеров портов, обрабатываемых определенным сервером.

По умолчанию Адреса не настроены.

Формат ip helper-address {server-address | Discarded}[dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]

Режим Interface Config

Параметр	Описание
server-address	Однонаправленный или направленный широковещательный IPv4, на который отправляются ретранслируемые пакеты UDP. Адрес сервера не может находиться в подсети на интерфейсе, где настроена запись ретранслятора, а также на любом интерфейсе локального маршрутизатора.
discard	Соответствующие пакеты не ретранслируются, а отклоняются, несмотря на записи глобальной конфигурации.
dest-udp-port	Номер UDP-порта назначения, от 0 до 65535.
port-name	Опционально порты UDP могут иметь свои имена. Порт может указываться как по имени, так и по номеру. Имена портов: • dhcp (порт 67) • domain (порт 53) • isakmp (порт 500) • mobile-ip (порт 434) • nameserver (порт 42) • netbios-dgm (порт 138) • netbios-ns (порт 137) • ntp (порт 123) • pim-auto-rp (порт 496) • rip (порт 520) • tacacs (порт 49)

Параметр	Описание
port-name	• tftp (порт 69) • time (порт 37) Остальные порты должны указываться по номеру.

ПРИМЕР: Для ретрансляции пакетов DHCP, полученных на интерфейсе 1/0/2, на два DHCP-сервера: 192.168.10.1 и 192.168.20.1 - используйте следующие команды:

```
(switch)#config
(switch)(config)#interface 1/0/2
(switch)(interface 1/0/2)#ip helper-address 192.168.10.1 dhcp
(switch)(interface 1/0/2)#ip helper-address 192.168.20.1 dhcp
```

ПРИМЕР: Для ретрансляции пакетов DHCP и DNS на адрес 192.168.30.1 используйте следующие команды:

```
(switch)#config
(switch)(config)#interface 1/0/2
(switch)(interface 1/0/2)#ip helper-address 192.168.30.1 dhcp
(switch)(interface 1/0/2)#ip helper-address 192.168.30.1 dns
```

ПРИМЕР: Эта команда имеет приоритет над командой «ip helper-address» в режиме global configuration. С данной конфигурацией агент ретранслятора пересылает: пакеты DHCP, полученные на любом интерфейсе, кроме 1/0/2 и 1/0/17, на адрес 192.168.40.1; пакеты DHCP и DNS, полученные на 1/0/2, на 192.168.40.2; SNMP traps (порт 162), полученные на интерфейсе 1/0/17, на 192.168.23.1; и отклоняет пакеты DHCP, полученные на 1/0/17.

```
(switch)#config
(switch)(config)#ip helper-address 192.168.40.1 dhcp
(switch)(config)#interface 1/0/2
(switch)(interface 1/0/2)#ip helper-address 192.168.40.2 dhcp
(switch)(interface 1/0/2)#ip helper-address 192.168.40.2 domain
(switch)(interface 1/0/2)#exit
(switch)(config)#interface 1/0/17
(switch)(interface 1/0/17)#ip helper-address 192.168.23.1 162
(switch)(interface 1/0/17)#ip helper-address discard dhcp
```

no ip helper-address (Interface Config)

Данная команда удаляет запись ретранслятора для интерфейса. Если команда выполняется без дополнительных аргументов, то удаляются все адреса IP Helper на этом интерфейсе.

Формат no ip helper-address [server-address [dest-udp-port | dhcp | domain | isakmp | mobileip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]

Режим Interface Config

ip helper enable

Данная команда включает ретрансляцию пакетов UDP. Команда может использоваться для временного отключения IP Helper без удаления адресов IP Helper. Эта команда заменяет команду bootpdhcprelay enable, но отвечает не только за пересылку пакетов DHCP, а также за все прочие протоколы, для которых настроены адреса IP Helper.

По умолчанию отключено

Формат ip helper enable

Режим Global Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(switch)(config)#ip helper enable
```

no ip helper enable

Данная команда отключает ретрансляцию пакетов UDP.

Формат no ip helper enable

Режим Global Config

show ip helper-address

Данная команда отображает конфигурацию адресов IP Helper. Аргумент *unit/slot/port* соответствует физическому интерфейсу маршрутизации либо интерфейсу маршрутизации VLAN. Ключевое слово vlan определяет VLAN ID маршрутизирующей VLAN напрямую вместо формата unit/slot/port.

Формат show ip helper-address [{unit/slot/port|vlan 1-4094}]

Режим Privileged EXEC

Параметр	Описание
interface	Конфигурация ретранслятора применяется к пакетам, получаемым на этом интерфейсе. Для глобальных записей IP helper в этом поле устанавливается значение any.
UDP Port	Конфигурация ретранслятора применяется к пакетам, UDP-портом назначения которых является этот порт. Записи, в которых UDP-порт прописан как «any», применяются к пакетом с UDP-портами назначения, перечисленными в таблице 4.
Discard	Если «Yes», то пакеты, получаемые на указанном интерфейсе с указанным портом назначения UDP, отклоняются вместо ретрансляции. Записи такого рода используются для создания исключений для глобальных записей.

Параметр	Описание
Hit Count	Количество раз, когда запись IP helper использовалась для того, чтобы переслать или отклонить пакет.
Server Address	IPv4-адрес сервера, на который ретранслируется пакет.

ПРИМЕР: Вывод командной строки для данной команды.

```
(switch) #show ip helper-address
IP helper is enabled
Interface       UDP Port        Discard   Hit Count       Server Address
-------------------------------------------------------------------------
1/0/1           dhcp            No        10              10.100.1.254
1/0/17          any             Yes       2               10.100.2.254
any             dhcp            No        0               10.200.1.254
```

show ip helper statistics

Данная команда отображает количество пакетов DHCP и прочих UDP-пакетов, обработанных и ретранслированных агентом UDP-ретранслятора.

Формат show ip helper statistics

Режим Privileged EXEC

Параметр	Описание
DHCP client messages received	Количество действительных сообщений, полученных от DHCP-клиента. Счетчик увеличивается только в том случае, если IP helper включен глобально, входящий интерфейс маршрутизации работает, а пакет проходит несколько проверок, таких как TTL>1, а также корректные IP-адреса источника и назначения.
DHCP client messages relayed	Количество сообщений DHCP-клиента, ретранслированных на сервер. Если пакет ретранслируется на несколько серверов, то каждый сервер увеличивает счетчик на 1.
DHCP server messages received	Количество DHCP-ответов, полученных от DHCP-сервера. Данный счетчик учитывает только одноадресные сообщения, отправляемые DHCP-сервером на агент ретранслятора для клиента.
DHCP server messages relayed	Количество сообщений DHCP-сервера, ретранслированных клиенту.

Параметр	Описание
UDP clients messages received	Количество полученных действительных UDP-пакетов. Счетчик учитывает сообщения как DHCP, так и других протоколов. Условия аналогичны тем, что описываются для первого статистического показателя в этой таблице.
UDP clients messages relayed	Количество ретранслированных действительных UDP-пакетов. Счетчик учитывает сообщения как DHCP, так и других протоколов. Счетчик увеличивается для каждого сервера, на который отправляется пакет.
DHCP message hop count exceeded max	Количество сообщений клиента DHCP, полученных с превышением максимального значения счетчика переходов. Это значение настраивается, ознакомиться с текущим значением можно при помощи команды «show bootpdhcprelay». Для каждой из этих ошибок приводится сообщение журнала. Агент DHCP-ретранслятора не пересылает эти пакеты.
DHCP message with secs field below min	Количество полученных сообщений клиента DHCP, поле «secs» которых меньше минимального значения. Значение «minimum secs» настраивается, ознакомиться с текущим значением можно при помощи команды «show bootpdhcprelay». Для каждой из этих ошибок приводится сообщение журнала. Агент DHCP-ретранслятора не пересылает эти пакеты.
DHCP message with giaddr set to local address	Количество полученных сообщений клиента DHCP, адрес шлюза, адрес агента ретрансляции (giaddr) которых совпадает с IP-адресом, настроенным на на одном из собственных интерфейсов ретранслятора. Скорее всего, это означает, что другое устройство пытается подделать адрес агента ретранслятора. Агент ретранслятора не пересылает эти пакеты. Для каждой из этих ошибок приводится сообщение журнала.
Packets with expired TTL	Количество пакетов, которые были получены с TTL равным 0 или 1 (но которые могли быть ретранслированы по всем своим прочим характеристикам).
Packets that matched a discard entry	Количество пакетов, проигнорированных агентом по причине того, что они соответствовали отклоняющей записи ретранслятора.

ПРИМЕР: Пример вывода командной строки для данной команды.

```
(switch)#show ip helper statistics
DHCP client messages received.....8
```

DHCP client messages relayed 2
DHCP server messages received 2
DHCP server messages relayed 2
UDP client messages received 8
UDP client messages relayed 2
DHCP message hop count exceeded max 0
DHCP message with secs field below min 0
DHCP message with giaddr set to local address 0
Packets with expired TTL 0
Packets that matched a discard entry 0

8.8. Команды ICMP Throttling

В этом разделе описаны команды, который используется для настройки параметров для передачи ICMP-сообщений различных типов.

ip unreachables

Данная команда позволяет генерировать сообщения ICMP Destination Unreachable на интерфейсе либо диапазоне интерфейсов. По умолчанию функция генерации сообщений ICMP Destination Unreachable включена.

По умолчанию Включено
Формат ip unreachables
Режим Interface Config

no ip unreachables

Данная команда отключает функцию генерации сообщений ICMP Destination Unreachable.

Формат no ip unreachables
Режим Interface Config

ip redirects

Данная команда позволяет маршрутизатору генерировать сообщения ICMP Redirect. По умолчанию функция генерации сообщений ICMP Redirect включена. Данная команда распространяет своё действие на интерфейс, диапазон интерфейсов или на все интерфейсы.

По умолчанию enable
Формат ip redirects
Режим Global Config
Interface Config

no ip redirects

Данная команда отключает функцию генерации сообщений ICMP Redirect.

Формат no ip redirects

Режимы Global Config

Interface Config

ip icmp echo-reply

Данная команда позволяет маршрутизатору генерировать сообщения ICMP Echo Reply. По умолчанию функция генерации сообщений ICMP Echo Reply включена.

По умолчанию Включено

Формат ip icmp echo-reply

Режим Global Config

no ip icmp echo-reply

Данная команда отключает функцию генерации сообщений ICMP Echo Reply.

Формат no ip icmp echo-reply

Режим Global Config

ip icmp error-interval

Данная команда ограничивает скорость отправки сообщений IPv4 ICMP error. Ограничение скорости настраивается как набор маркеров с двумя настраиваемыми параметрами: burst-size и burst-interval.

Параметр burst-interval определяет частоту инициализации набора маркетов с маркерами burst-size. Значение burst-interval принадлежит диапазону от 0 до 2147483647 миллисекунд (мс). Параметр burst-size представляет собой количество сообщений ICMP, которые могут быть отправлены за один burst-interval. Диапазон: 1 – 200 сообщений. Для отмены ограничений скорости установите burst-interval на ноль (0).

По умолчанию burst-interval: 1000 мс.

burst-size: 100 сообщений

Формат ip icmp error-interval burst-interval [burst-size]

Режим Global Config

no ip icmp error-interval

Данная команда возвращает параметрам burst-interval и burst-size значения по умолчанию.

Формат no ip icmp error-interval

Режим Global Config

9. КОМАНДЫ УПРАВЛЕНИЯ IPV6

В этом разделе описываются команды IPv6, доступные в интерфейсе командной строки коммутатора. Раздел состоит из следующих глав:

- Команды управления IPv6
- Команды DHCPv6

ВНИМАНИЕ: В ДАННОМ РАЗДЕЛЕ КОМАНДЫ ДЕЛЯТСЯ НА ТРИ ФУНКЦИОНАЛЬНЫЕ ГРУППЫ:

Команды Show отображают настройки коммутатора, статистику и прочую информацию.

Команды конфигурации вносят изменения в настройки коммутатора. Каждой команде конфигурации соответствует команда информации, показывающая текущие настройки.

Команды Clear сбрасывают определенные настройки на заводские значения.

9.1. Команды управления IPv6

Команды управления Pv6 позволяют управлять коммутатором как через адрес IPv6, так и через адрес IPv4 (то есть независимо от маршрутизации IPv6). Для маршрутизации/IPv6 включена поддержка работы с IPv4/IPv6 через служебный порт коммутатора. Коммутатор имеет такие возможности, как:

Статическое назначение адресов IPv6 и шлюзов для служебных и сетевых портов.

Возможность отправки ping на локальный адрес IPv6 через служебный или сетевой порт.

Используя команды управления IPv6, вы можете отправлять SNMP trap и запросы через служебный или сетевой порт.

Пользователь может управлять устройством через сетевой порт (в дополнение к интерфейсу маршрутизации или служебному порту).

network ipv6 enable

Данная команда используется для включения IPv6 на сетевом порте. По умолчанию работа IPv6 на сетевых портах включена.

По умолчанию включено

Формат network ipv6 enable

Режим Privileged EXEC

no network ipv6 enable

Данная команда используется для отключения IPv6 на сетевом порте.

Формат no network ipv6 enable

Режим Privileged EXEC

network ipv6 address

Используйте параметры этой команды, чтобы вручную настроить глобальный адрес IPv6; включить или отключить автоконфигурирование глобальных адресов без учета состояния; включить или отключить информацию протокола клиента dhcpv6 для сетевого порта. На сетевом порте можно настроить несколько адресов IPv6.

Формат network ipv6 address {*address/prefix-length* [eui64] | autoconfig | dhcp}

Режим Privileged EXEC

Параметр	Описание
address	IPv6-префикс в глобальном формате адреса IPv6.
prefix-length	Значение длины префикса IPv6.
eui64	Сформулируйте адрес IPv6 в формате eui64.
autoconfig	Настройте возможности stateless-конфигурации глобальных адресов.
dhcp	Настройте протокол клиента dhcpv6.

no network ipv6 address

Данная команда удаляет все настроенные префиксы IPv6.

Используйте эту команду с опцией «**address**», чтобы удалить настроенный вручную глобальный адрес IPv6 на интерфейсе сетевого порта.

Используйте эту команду с опцией «**autoconfig**», чтобы отключить stateless-автоконфигурацию глобального адресата на сетевом порте.

Эта команда с опцией «**dhcp**» отключает клиентский протокол dhcpv6 на сетевом порте.

Формат no network ipv6 address {*address/prefix-length* [eui64] | autoconfig | dhcp}

Режим Privileged EXEC

network ipv6 gateway

Данная команда используется для настройки шлюза IPv6 (маршрутизатора по умолчанию) для сетевого порта.

Формат network ipv6 gateway *gateway-address*

Режим Privileged EXEC

Параметр	Описание
gateway-address	Адрес шлюза IPv6 в формате global или link-local.

no network ipv6 gateway

Данная команда используется для удаления шлюзов IPv6 на сетевом порте.

Формат no network ipv6 gateway

Режим Privileged EXEC

network ipv6 neighbor

Используйте эту команду, чтобы вручную добавить соседей IPv6 в таблицу соседей IPv6 для этого сетевого порта. Если сосед IPv6 уже существует, запись автоматически преобразуется в статическую. Статические записи не изменяются процессом обнаружения соседей. Тем не менее, в случае пересылки IPv6 они обрабатываются одинаково.

Формат network ipv6 neighbor *ipv6-address macaddr*

Режим Privileged EXEC

Параметр	Описание
ipv6-address	IPv6-адрес соседа или интерфейса.
macaddr	Адрес link-layer.

no network ipv6 neighbor

Данная команда удаляет соседей IPv6 из соответствующей таблицы.

Формат no network ipv6 neighbor *ipv6-address macaddr*

Режим Privileged EXEC

show network ipv6 neighbors

Данная команда отображает информацию о записях соседей IPv6, сохраненных в кэше сетевого порта.

По умолчанию Нет

Формат show network ipv6 neighbors

Режим Privileged EXEC

Поле	Описание
IPv6 Address	IPv6-адрес соседа.
MAC Address	MAC-адрес соседа.
isRtr	Показывает, является ли сосед маршрутизатором. TRUE – является; FALSE – нет.
Neighbor State	Состояние записи кэша соседей. Возможные значения: Incomplete, Reachable, Stale, Delay, Probe и Unknown
Age	Время в секундах, прошедшее с момента добавления записи в кэш.
Last Updated	Время в секундах, прошедшее с момента добавления записи в кэш.

Поле	Описание
Type	Тип записи. «Static» - запись настроена вручную, «Dynamic» - запись создана динамически.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) #show network ipv6 neighbors
IPv6 Address                MAC Address        Neighbor isRtr State    Age (Secs)  Type
--------------------------------------------------------------------------------
FE80::5E26:AFF:FEBD:852C    5c:26:0a:bd:85:2c  FALSE Reachable         0           Static
```

ping ipv6

Данная команда позволяет определить доступность другого компьютера в сети. Пинг инициируется из командной строки либо Веб-интерфейса, и предполагает синхронный ответ. Чтобы использовать эту команду, настройте коммутатор для сетевого (внутриполосного) соединения. У исходного и целевого устройств должна быть включена утилита ping, запущенная поверх TCP/IP. Запрос ping может быть отправлен на коммутатор с любой рабочей станции IP, с которой коммутатор соединен через VLAN по умолчанию (VLAN 1), пока существует физический путь между коммутатором и рабочей станцией. Интерфейс терминала посылает три пинга на целевую станцию. Параметр the **ipv6-address|hostname** – отправить запрос ping на интерфейс, используя его глобальный адрес IPv6. Аргумент «unit/slot/port» соответствует физическому интерфейсу маршрутизации либо интерфейсу маршрутизации VLAN. Ключевое слово **vlan** определяет VLAN ID маршрутизирующей VLAN напрямую вместо формата **unit/slot/port**. Необязательное ключевое слово **size** указывает размер пакета ping.

Вы можете использовать службы ping и traceroute через сервисные или сетевые порты, если вы используете глобальный адрес IPv6 **ipv6-global-address|hostname**. Любые назначения глобального IP-адреса или шлюза IPv6 для этих интерфейсов приведут к тому, что маршруты IPv6 будут установлены в IP-стеке, так что запрос ping или traceroute будет правильно перенаправлен на порт службы/сети. При обращении к адресу IPv6 link-local, вы также должны указать интерфейс службы или сетевого порта, используя параметр *serviceport* или *network*.

По умолчанию count: 1

interval: 3 (секунды)

size: 0 (байт).

Формат ping ipv6 {ipv6-global-address|hostname | interface network link-local-address} [size datagram-size]

Режим Privileged EXEC

User EXEC

Ключевое слово	Описание
interface	Ключевое слово *interface* используется для отправки запроса ping на интерфейс, с использованием его глобального адреса IPv6 либо адреса link-local.
size	Необязательное ключевое слово *size* указывает размер пакета ping.
ipv6-address	Адреса link local IPv6 устройства, на которое отправляется запрос.

9.2. Команды DHCPv6

В этом разделе описаны команды, используемые для просмотра информации DHCPv6.

show network ipv6 dhcp statistics

Данная команда отображает статистику клиента DHCPv6, работающего на интерфейсе сетевого управления.

Формат show network ipv6 dhcp statistics

Режим Privileged EXEC

User EXEC

Поле	Описание
DHCPv6 Advertisement Packets Received	Количество пакетов DHCPv6 Advertisement, полученных на интерфейсе.
DHCPv6 Reply Packets Received	Количество пакетов DHCPv6 Reply, полученных на интерфейсе.
Received DHCPv6 Advertisement Packets Discarded	Количество пакетов DHCPv6 Advertisement, отклоненных на интерфейсе.
Received DHCPv6 Reply Packets Discarded	Количество пакетов DHCPv6 Reply, отклоненных на интерфейсе.
DHCPv6 Malformed Packets Received	Количество поврежденных пакетов DHCPv6, полученных на интерфейсе.

Поле	Описание
Total DHCPv6 Packets Received	Общее количество пакетов DHCPv6, полученных на интерфейсе.
DHCPv6 Solicit Packets Transmitted	Количество пакетов DHCPv6 Solicit, отправленных на интерфейсе.
DHCPv6 Request Packets Transmitted	Количество пакетов DHCPv6 Request, отправленных на интерфейсе.
DHCPv6 Renew Packets Transmitted	Количество пакетов DHCPv6 Renew, отправленных на интерфейсе.
DHCPv6 Rebind Packets Transmitted	Количество пакетов DHCPv6 Rebind, отправленных на интерфейсе.
DHCPv6 Release Packets Transmitted	Количество пакетов DHCPv6 Release, отправленных на интерфейсе.
Total DHCPv6 Packets Transmitted	Общее количество пакетов DHCPv6, отправленных на интерфейсе.

ПРИМЕР: Пример вывода командной строки для данной команды.

```
(admin)#show network ipv6 dhcp statistics
DHCPv6 Client Statistics
------------------------
DHCPv6 Advertisement Packets Received .....0
DHCPv6 Reply Packets Received.....0
Received DHCPv6 Advertisement Packets Discarded .....0
Received DHCPv6 Reply Packets Discarded.....0
DHCPv6 Malformed Packets Received .....0
Total DHCPv6 Packets Received .....0
DHCPv6 Solicit Packets Transmitted.....0
DHCPv6 Request Packets Transmitted.....0
DHCPv6 Renew Packets Transmitted .....0
DHCPv6 Rebind Packets Transmitted .....0
DHCPv6 Release Packets Transmitted.....0
```

Total DHCPv6 Packets Transmitted 0

clear network ipv6 dhcp statistics

Данная команда используется для очистки статистики DHCPv6 на интерфейсе сетевого управления.

Формат clear network ipv6 dhcp statistics

Режим Privileged EXEC

9.3. Команды конфигурации DHCPv6 Snooping

В этом разделе описаны команды, которые используются для настройки IPv6 DHCP Snooping.

ipv6 dhcp snooping

Данная команда глобально включает IPv6 DHCP Snooping.

По умолчанию отключено

Формат ipv6 dhcp snooping

Режим Global Config

no ipv6 dhcp snooping

Данная команда глобально отключает IPv6 DHCP Snooping.

Формат no ipv6 dhcp snooping

Режим Global Config

ipv6 dhcp snooping vlan

Данная команда включает DHCP snooping для списка VLAN (разделяются запятыми).

По умолчанию отключено

Формат ipv6 dhcp snooping vlan vlan-list

Режим Global Config

no ipv6 dhcp snooping vlan

Данная команда отключает DHCP Snooping на VLAN.

Формат no ipv6 dhcp snooping vlan *vlan-list*

Режим Global Config

ipv6 dhcp snooping verify mac-address

Данная команда используется для включения функции сверки MAC-адреса источника с MAC-адресом клиента в полученных сообщениях DCHP.

По умолчанию включено

Формат ipv6 dhcp snooping verify mac-address

Режим Global Config

no ipv6 dhcp snooping verify mac-address

Данная команда используется для отключения функции сверки MAC-адреса источника с MAC-адресом клиента.

Формат no ipv6 dhcp snooping verify mac-address

Режим Global Config

ipv6 dhcp snooping database

Данная команда настраивает постоянное местоположение базы данных DHCP Snooping. Это может быть как локальный, так и удалённый файл (на устройстве с указанным IP).

По умолчанию local

Формат ipv6 dhcp snooping database {local|tftp://hostIP/filename}

Режим Global Config

ip dhcp snooping database write-delay

Данная команда настраивает интервал (в секундах), с которым будет сохраняться база данных DHCP Snooping. Диапазон времени: 15 – 86400 секунды.

По умолчанию 300 секунд

Формат ip dhcp snooping database write-delay in seconds

Режим Global Config

no ip dhcp snooping database write-delay

Данная команда сбрасывает настройки задержки записи на значения по умолчанию.

Формат no ip dhcp snooping database write-delay

Режим Global Config

ipv6 dhcp snooping binding

Данная команда позволяет настроить статическую привязку DHCP Snooping.

Формат ipv6 dhcp snooping binding mac-address vlan vlan id ip address interface interface id

Режим Global Config

no ipv6 dhcp snooping binding

Данная команда удаляет статическую запись DHCP из базы данных DHCP Snooping.

Формат no ipv6 dhcp snooping binding *mac-address*

Режим Global Config

ipv6 dhcp snooping trust

Данная команда настраивает интерфейс или диапазон интерфейсов в качестве доверенного.

По умолчанию отключено

Формат ipv6 dhcp snooping trust

Режим Interface Config

no ipv6 dhcp snooping trust

Данная команда настраивает порт как недоверенный.

Формат no ipv6 dhcp snooping trust

Режим Interface Config

ipv6 dhcp snooping log-invalid

Данная команда позволяет настроить логирование фильтрации DHCP-сообщений при помощи приложения DHCP Snooping. Команда может использоваться для настройки как одного интерфейса, так и диапазона интерфейсов.

По умолчанию отключено

Формат ipv6 dhcp snooping log-invalid

Режим Interface Config

no ipv6 dhcp snooping log-invalid

Данная команда отключает логирование фильтрации DHCP-сообщений при помощи приложения DHCP Snooping.

Формат no ipv6 dhcp snooping log-invalid

Режим Interface Config

ipv6 dhcp snooping limit

Данная команда используется для настройки скорости, с которой сообщения DHCP Snooping поступают на интерфейс или диапазон интерфейсов. Отключено по умолчанию. При включении скорость может быть настроена в диапазоне от 0 до 300 пакетов в секунду. Диапазон первышения: от 1 до 15 секунд. Ограничение скорости, настроеное на физическом порте, может быть применено как к доверенным, так и к недоверенным портам.

По умолчанию отключено (без лимита)

Формат ipv6 dhcp snooping limit {rate pps [burst interval seconds]}

Режим Interface Config

no ipv6 dhcp snooping limit

Данная команда используется для сброса скорости отправки сообщений DHCP Snooping и первышения на значения по умолчанию.

Формат no ipv6 dhcp snooping limit

Режим Interface Config

ipv6 verify source

Данная команда позволяет настроить атрибут защиты источника (IPv6SG) ID источника для аппаратной фильтрации трафика. ID источника представляет собой комбинацию из IP- и MAC-адресов. Обычная команда позволяет фильтровать трафик на основе IP-адреса. С опцией «port-security» трафик фильтруется на основе IP- и MAC-адресов.

Команда может использоваться для настройки как одного интерфейса, так и диапазона интерфейсов.

По умолчанию ID источника совпадает с IP-адресом

Формат ipv6 verify source {port-security}

Режим Interface Config

no ipv6 verify source

Данная команда отключает конфигурацию IPv6SG на коммутаторе. Невозможно отключить только port-security, если она настроена.

Формат no ipv6 verify source

Режим Interface Config

ipv6 verify binding

Данная команда используется для настройки записей защиты источника IPv6 (IPv6SG).

Формат pv6 verify binding *mac-address* vlan *vlan id ipv6 address* interface *interface id*

Режим Global Config

no ipv6 verify binding

Данная команда удаляет статическую запись IPv6SG из базы данных IPv6SG.

Формат no ipv6 verify binding mac-address vlan vlan id ipv6 address interface interface id

Режим Global Config

show ipv6 dhcp snooping

Данная команда отображает настройки DHCP Snooping: глобальные и для конкретных портов.

Формат show ipv6 dhcp snooping

Режим Privileged EXEC

Термин	Значение
Interface	Интерфейс, для которого отображаются данные.

Термин	Значение
Trusted	Если этот параметр включен, DHCP snooping считает этот порт доверенным. По умолчанию - выключен.
Log Invalid Pkts	Если этот параметр включен, приложение DHCP snooping журналирует некорректные пакеты на указанном интерфейсе.

ПРИМЕР: Пример вывода командной строки для данной команды.

```
(switch) #show ipv6 dhcp snooping
DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled DHCP snooping is enabled on the following VLANs: 11 - 30, 40
Interface                Trusted                  Log Invalid Pkts
-----------------------------------------------------------------------------
0/1                      Yes                      No
0/2                      No                       Yes
0/3                      No                       Yes
0/4                      No                       No
0/6                      No                       No
```

show ipv6 dhcp snooping binding

Данная команда отображает записи привязки DHCP Snooping. Для ограничения вывода команды используйте следующие параметры:

Dynamic: Ограничить вывод на основе DCHP snooping.

Interface: Ограничить вывод на основе указанного интерфейса.

Static: Ограничить вывод на основе статических записей.

VLAN: Ограничить вывод на основе VLAN.

Формат show ipv6 dhcp snooping binding [{static/dynamic}] [interface unit/slot/port] [vlan id]

Режим Privileged EXEC

Термин	Значение
MAC Address	Отображает MAC-адрес, добавленный для привязки. MAC-адрес - это ключевой параметр базы данных привязки.
IPv6 Address	Отображает действительный IPv6-адрес правила привязки.
VLAN	VLAN правила привязки.

Термин	Значение
Interface	Интерфейс для добавления привязки к интерфейсу DHCP snooping.
Type	Тип привязки: динамическая или статически настроенная при помощи командной строки.
Lease (sec)	Оставшееся время аренды для записи.

ПРИМЕР: Пример вывода командной строки для данной команды.

```
(switch) #show ipv6 dhcp snooping binding

Total number of bindings: 2

MAC Address       IPv6 Address    VLAN    Interface    Type    Lease time (Secs)
-------------------------------------------------------------------------------
00:02:B3:06:60:80 2000::1/64      10      0/1                  86400
00:0F:FE:00:13:04 3000::1/64      10      0/1                  86400
```

show ipv6 dhcp snooping database

Данная команда отображает конфигурацию DHCP Snooping, имеющую отношение к постоянному хранению базы данных.

Формат show ipv6 dhcp snooping database

Режим Privileged EXEC

Термин	Значение
Agent URL	URL агента базы данных привязки.
Термин	Значение
Write Delay	Максимальное время записи базы данных на локальное или удаленное хранилище.

ПРИМЕР: Пример вывода командной строки для данной команды.

```
(switch) #show ipv6 dhcp snooping database agent url: /10.131.13.79:/sai1.txt write-delay: 5000
```

show ipv6 dhcp snooping interfaces

Данная команда отображает состояние IGMP snooping указанного интерфейса либо всех интерфейсов.

ПРИМЕР: Пример вывода командной строки для данной команды.

(switch) #show ipv6 dhcp snooping interfaces

Interface	Trust State	Rate Limit (pps)	Burst Interval (seconds)
1/g1	No	15	1
1/g2	No	15	1
1/g3	No	15	1

(switch) #show ip dhcp snooping interfaces ethernet 1/0/1

Interface	Trust State	Rate Limit (pps)	Burst Interval (seconds)
1/0/1	Yes	15	1

show ipv6 dhcp snooping statistics

Данная команда отображает статистику нарушений безопасности IPv6 DHCP Snooping на недоверенных портах.

ПРИМЕР: Пример вывода командной строки для данной команды.

(switch) #show ipv6 dhcp snooping statistics

Interface	MAC Verify	Client Ifc	DHCP Server	Failures	Mismatch	Msgs Rec'd
1/0/2	0	0	0			
1/0/3	0	0	0			
1/0/4	0	0	0			
1/0/5	0	0	0			
1/0/6	0	0	0			
1/0/7	0	0	0			
1/0/8	0	0	0			
1/0/9	0	0	0			
1/0/10	0	0	0			
1/0/11	0	0	0			
1/0/12	0	0	0			
1/0/13	0	0	0			
1/0/14	0	0	0			
1/0/15	0	0	0			

1/0/16	0	0	0
1/0/17	0	0	0
1/0/18	0	0	0
1/0/19	0	0	0
1/0/20	0	0	0

clear ipv6 dhcp snooping binding

Данная команда удаляет все привязки DHCPv6 Snooping на всех интерфейсах (либо на указанном интерфейсе).

clear ipv6 dhcp snooping statistics

Данная команда очищает всю статистику DHCPv6 Snooping.

Формат clear ipv6 dhcp snooping statistics

Режим Privileged EXEC

show ipv6 verify

Данная команда отображает конфигурацию IPv6 указанного интерфейса.

Формат show ipv6 verify interface

Режим Privileged EXEC

Термин	Значение
Interface	Интерфейс в формате unit/slot/port.
Filter Type	Одно из двух значений: • ip-v6mac: На этом интерфейсе настроена фильтрация по MAC. • ipv6: На этом интерфейсе настроена только фильтрация адресов IPv6.
IPv6 Address	IPv6-адрес интерфейса
MAC Address	Если на интерфейсе не настроена фильтрация по MAC, это поле остается пустым. Если на интерфейсе отключена функция «port security», в этом поле отображается «permit-all».
VLAN	VLAN для правила привязки.

ПРИМЕР: Пример вывода командной строки для данной команды.

```
(switch) #show ipv6 verify 0/1
```

```
Interface       Filter Type     IP Address          MAC Address         Vlan
-------------------------------------------------------------------------------
0/1             ipv6-mac        2000::1/64          00:02:B3:06:60:80   10
0/1             ipv6-mac        3000::1/64          00:0F:FE:00:13:04   10
```

show ipv6 verify source

Данная команда отображает конфигурацию IPv6SG для всех портов. Если указан интерфейс, то выводится информация только для указанного unit/slot/port.

Формат show ipv6 verify source {interface}

Режим Privileged EXEC

Термин	Значение
Interface	Интерфейс в формате unit/slot/port.
Filter Type	Одно из двух значений: • ip-v6mac: На этом интерфейсе настроена фильтрация по MAC. • ipv6: На этом интерфейсе настроена только фильтрация адресов IPv6.
IPv6 Address	IPv6-адрес интерфейса
MAC Address	Если на интерфейсе не настроена фильтрация по MAC, это поле остается пустым. Если на интерфейсе отключена функция «port security», в этом поле отображается «permit-all».
VLAN	VLAN для правила привязки.

ПРИМЕР: Пример вывода командной строки для данной команды.

```
(switch) #show ipv6 verify source
Interface       Filter Type     IP Address          MAC Address         Vlan
-------------------------------------------------------------------------------
0/1             ipv6-mac        2000::1/64          00:02:B3:06:60:80   10
0/1             ipv6-mac        3000::1/64          00:0F:FE:00:13:04   10
```

show ipv6 source binding

Данная команда отображает привязки IPv6SG.

Формат show ipv6 source binding [{dhcp-snooping|static}] [interface unit/slot/port] [vlan id]

Режим Privileged EXEC

Термин	Значение
MAC Address	MAC-адрес для добавленной записи.
IP Address	IP-адрес для добавленной записи.
Type	Тип записи: статическая (настроенная из командной строки) или динамическая (полученная при помощи DHCP Snooping).
VLAN	Сеть VLAN для записи.
Interface	IP-адрес интерфейса в формате *unit/slot/port*.

ПРИМЕР: Пример вывода командной строки для данной команды.

```
(switch) #show ipv6 source binding
MAC Address       IP Address   Type            Vlan      Interface
-------------------------------------------------------------------------
00:00:00:00:00:08 2000::1      dhcp-snooping   2         1/0/1
00:00:00:00:00:09 3000::1      dhcp-snooping   3         1/0/1
00:00:00:00:00:0A 4000::1      dhcp-snooping   4         1/0/1
```

10. КОМАНДЫ QUALITY OF SERVICE

В этом разделе описываются команды Quality of Service (QoS), доступные в интерфейсе командной строки коммутатора.

Раздел состоит из следующих глав:

ПРИМЕЧАНИЕ: В данном разделе команды делятся на две функциональные групы:

Команды Show отображают настройки коммутатора, статистику и прочую информацию.

Команды конфигурации вносят изменения в настройки коммутатора. Каждой команде конфигурации соответствует команда информации, показывающая текущие настройки.

10.1. Команды Class of Service

В этом разделе описаны команды, который используется для настройки и просмотра конфигурации Class of Service (CoS). Команды из этого раздела позволяют контролировать приоритеты и скорость передачи трафика.

ПРИМЕЧАНИЕ: Действие команд в режиме Interface Config распространяется на один интерфейс. Действие команд в режиме Global Config распространяется на все интерфейсы.

classofservice dot1p-mapping

Данная команда сопоставляет приоритет 802.1p с внутренними классами трафика. Диапазон значений **userpriority**: 0 – 7. Диапазон значений **trafficclass**: 0 – 7.

Формат classofservice dot1p-mapping userpriority trafficclass

Режимы Global Config

Interface Config

no classofservice dot1p-mapping

Данная команда сопоставляет приоритет 802.1p со значениями внутренних классов трафика по умолчанию.

Формат no classofservice dot1p-mapping

Режимы Global Config

Interface Config

classofservice ip-dscp-mapping

Данная команда сопоставляет значение IP DSCP с внутренними классами трафика. Значение *ipdscp* указывается либо как целое число от 0 до 63, либо символически, через одно из следующих ключевых слов: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

Диапазон значений *trafficclass*: 0 – 7.

Формат classofservice ip-dscp-mapping ipdscp trafficclass

Режим Global Config

no classofservice ip-dscp-mapping

Данная команда сопоставляет каждое значение IP DSCP со значениями внутренних классов трафика по умолчанию.

Формат no classofservice ip-dscp-mapping

Режим Global Config

classofservice trust

Данная команда устанавливает доверенный режим class of service на интерфейсе или диапазоне интерфейсов. Вы можете установить режим, чтобы доверять одному из маркеров: Dot1p (802.1p), IP DSCP или IP Precedence. Также вы можте установить недоверенный режим на интерфейсе. Если вы настраиваете интерфейс для использования Dot1p, режим не появляется в выводе команды **show running-config**, поскольку Dot1p является значением по умолчанию.

По умолчанию dot1p

Формат classofservice trust {dot1p | ip-dscp | untrusted}

Режимы Global Config

Interface Config

no classofservice trust

Данная команда сбрасывает режим интерфейса на настройки по умолчанию.

Формат no classofservice trust

Режимы Global Config

Interface Config

cos-queue min-bandwidth

Данная команда определяет минимальную гарантированную полосу пропускания для каждой очереди на интерфейсе, диапазоне интерфейсов или на всех интерфейсах. Для каждой поддерживаемой очереди должно быть указано значение от 0 до 100 (процент от

скорости передачи), где 0 - отсутствие гарантированной минимальной полосы пропускания. Сумма всех указанных значений не должна превышать 100.

Формат cos-queue min-bandwidth bw-0 bw-1 … bw-n

Режимы Global Config

Interface Config

no cos-queue min-bandwidth

Данная команда возвращает значения по умолчанию для минимально гарантированного значения для каждой очереди.

Формат no cos-queue min-bandwidth

Режимы Global Config

Interface Config

cos-queue strict

Данная команда активирует режим строгой приоритизации для каждой конкретной очереди на интерфейсе, диапазоне интерфейсов или на всех интерфейсах.

Формат cos-queue strict queue-id-1 [queue-id-2 … queue-id-n]

Режимы Global Config

Interface Config

no cos-queue strict

Данная команда возвращает значения по умолчанию для режима строгой приоритизации.

Формат no cos-queue strict queue-id-1 [queue-id-2 … queue-id-n]

Режимы Global Config

Interface Config

show classofservice dot1p-mapping

Эта команда отображает текущее сопоставление приоритетов Dot1p (802.1p) с внутренними классами трафика для определенного интерфейса. Параметр **unit/slot/port** является необязательным и присутствует только на платформах, которые поддерживают независимое сопоставление class of service для каждого порта. Если параметр указан, отображается таблица сопоставления 802.1p указанного интерфейса. Если не указан - отображаются последние глобальные параметры конфигурации. Для получения дополнительной информации см. раздел "Команды Voice VLAN".

Формат show classofservice dot1p-mapping [unit/slot/port]

Режим Privileged EXEC

Следующая информация выводится для каждого приоритета пользователя.

Термин	Значение
User Priority	Значение приоритета пользователя 802.1p.

Термин	Значение
Traffic Class	Внутренний идентификатор класса трафика, с которым сопоставляется пользовательское значение приоритета.

show classofservice ip-dscp-mapping

Эта команда отображает текущее сопоставление приоритетов IP DSCP с внутренними классами трафика для глобальной конфигурации.

Формат show classofservice ip-dscp-mapping

Режим Privileged EXEC

Следующая информация выводится для каждого приоритета пользователя.

Термин	Значение
IP DSCP	Значение IP DSCP.
Traffic Class	Внутренний идентификатор класса трафика, с которым сопоставляется пользовательское значение приоритета.

show classofservice trust

Команда отображает режим доверия для определенного интерфейса. Параметр **unit/slot/port** является необязательным и присутствует только на платформах, которые поддерживают независимое сопоставление class of service для каждого порта. При указании интерфейса команда отображает режим для него. Если он не указан - отображаются последние глобальные параметры конфигурации.

Формат show classofservice trust [unit/slot/port]

Режим Privileged EXEC

Термин	Значение
Class of Service Trust Mode	Режим доверенности, может быть Dot1P, IP DSCP либо Untrusted (недоверенный).
Non-IP Traffic Class	Класс, используемый для не-IP-трафика (только для режима IP DSCP).
Untrusted Traffic Class	Класс, используемый для всего недоверенного трафика (только режим Untrusted).

show interface cos-queue

Данная команда отображает настройки очереди CoS для указанного интерфейса. Параметр **unit/slot/port** является необязательным и присутствует только на платформах, которые поддерживают независимое сопоставление class of service для каждого порта.

Если параметр указан, то отображается таблица сопоставления 802.1p указанного интерфейса. Если не указан - отображаются последние глобальные параметры конфигурации.

Формат show interfaces cos-queue [unit/slot/port]

Режим Privileged EXEC

Термин	Значение
Queue Id	Интерфейс поддерживает n очередей, нумеруемых от 0 до (n-1). Значение n зависит от конкретной платформы.
Minimum Bandwidth	Минимальная пропускная способность передачи для очереди, выраженная в процентах. Значение 0 означает, что пропускная способность не гарантируется. Это настроенное значение.
Scheduler Type	Механизм планировщика для этой очереди: строгий приоритет или средневзвешенная схема. Это настраиваемое значение.
Queue Management Type	Методика управления глубиной очереди, используемая для этой очереди (tail drop).

Если указан интерфейс, команда также отображает следующую информацию.

Термин	Значение
Interface	**unit/slot/port** интерфейса. При отображении глобальной конфигурации эта строка вывода заменяется индикацией Global Config.
Interface Shaping Rate	Максимальный предел пропускной способности для интерфейса в целом. Он не зависит от значений максимальной пропускной способности очереди для интерфейса. Это настроенное значение.

10.2. Команды Differentiated Services

В этом разделе описаны команды, используемые для настройки дифференцированных служб QOS (DiffServ).

DiffServ настраивается в несколько этапов. Необходимо настроить три компонента DiffServ.

Класс (class)

1. Создание и удаление классов.
   1.1. Определение критериев отбора для класса.
2. Политика (policy)
   2.1. Создание и удаление политик
   2.2. Связывание класса с политикой

2.3. Определение инструкций политики для комбинации политики и класса

3. Служба (service)

3.1. Добавление политик на входящий интерфейс и удаление из него.

Класс DiffServ определяет критерии фильтрации пакетов. Атрибуты политики DiffServ определяют способ, которым коммутатор обрабатывает пакеты. Вы можете определить атрибуты политики для каждого экземпляра класса. Коммутатор применяет эти атрибуты при обнаружении совпадения.

Обработка пакетов начинается, когда коммутатор проверяет пакет на соответствие критериям. Коммутатор применяет политику к пакету, когда находит соответствие классу в этой политике.

При создании класса DiffServ применяются следующие правила:

- Каждый класс может содержать максимум один дочерний (вложенный) класс
- Определения классов не поддерживают иерархические политики обслуживания

Заданное определение класса может содержать максимум одну ссылку на другой класс. Вы можете комбинировать ссылку с другими критериями соответствия. Класс, на который ссылаются, действительно является ссылкой, а не копией, так как дополнения к этому классу влияют на все классы, которые ссылаются на него. Изменения в любых определениях класса, на который в настоящее время ссылается любой другой класс, должны приводить к верным определениям классов для всех производных классов, иначе коммутатор отклоняет изменение. Вы можете удалить ссылку на класс из определения класса.

Единственный способ удалить индивидуальный критерий соответствия из существующего определения класса - удалить класс и повторно создать его.

ПРИМЕЧАНИЕ: Возможности маркировки для политик включают CoS, IP DSCP и IP Precedence. Хотя последние два имеют смысл только для пакетов IP-типов, маркировка CoS разрешена как для IP, так и для не-IP-пакетов, поскольку она обновляет поле приоритета пользователя 802.1p, содержащееся в теге VLAN заголовка пакета уровня 2 OSI.

diffserv

Данная команда включает активный (active) режим работы DiffServ. При отключении конфигурация DiffServ не удаляется и остаётся доступной для редактирования. При включении активируются службы DiffServ.

Формат diffserv

Режим Global Config

no diffserv

Данная команда отключает активный (active) режим работы DiffServ и переводит его в неактивный режим. При отключении конфигурация DiffServ не удаляется и остаётся доступной для редактирования. При включении активируются службы DiffServ.

Формат no diffserv

Режим Global Config

10.3. Команды классов DiffServ

Данные команды используются для определения классификации трафика. Для классификации трафика указывается совокупность действий, основанная на DSCP и классах траффика (имя, критерий совпадения).

Этот набор команд состоит из создания/удаления класса и его критериев отбора, включая команды отбора классов, определяющие критерии уровня 3, уровня 2 и общий критерий отбора. Критерии соответствия классу (правила класса) с определением класса, состоящим из одного или нескольких правил для идентификации трафика, принадлежащего классу.

ПРИМЕЧАНИЕ: После создания критерия соответствия классу его невозможно изменить или удалить. Чтобы изменить или удалить критерий соответствия классу, необходимо удалить и заново создать весь класс.

Корневая команда – **class-map**.

class-map

Данная команда определяет класс DiffServ типа match-all. Если не указаны условия соответствия, команда входит в режим «**class-map**». Имя класса **class-map-name** – это строка из букв и цифр длиной от 1 до 31 символа (чувствительно к регистру), которая является уникальным идентификатором класса DiffServ.

ПРИМЕЧАНИЕ: Имя «**default**» зарезервировано системой и не подходит в качестве имени пользовательского класса.

Класс типа match-all указывает на то, что пакет должен удовлетворять всем условиям, чтобы быть признанным членом класса. Эта команда может использоваться без указания типа класса для входа в режим Class-Map Config для существующего класса DiffServ.

ПРИМЕЧАНИЕ: Необязательное ключевое слово ipv4 определяет протокол уровня 3 OSI для данного класса. Если он не указан, параметр использует значение ipv4 по умолчанию.

ПРИМЕЧАНИЕ: Режим CLI изменяется на Class-Map Config, при успешном выполнении данной команды.

Формат class-map match-all class-map-name {ipv4}

Режим Global Config

no class-map

Данная команда удаляет существующий класс DiffServ. Параметр **class-map-name** – имя существующего класса DiffServ. (Имя «default» зарезервировано системой и не подходит в качестве имени пользовательского класса.) Эта команда может быть вызвана в любое время; если на класс в настоящее время ссылается одна или несколько политик или любой другой класс, действие удаления не выполняется.

Формат no class-map *class-map-name*

Режим Global Config

class-map rename

Данная команда изменяет имя класса DiffServ. Параметр **class-map-name** – имя существующего класса DiffServ. Параметр **new-class-map-name** – это строка из букв и

цифр длиной от 1 до 31 символа (чувствительно к регистру), которая является уникальным идентификатором класса DiffServ.

По умолчанию нет

Формат class-map rename class-map-name new-class-map-name

Режим Global Config

match ethertype

Эта команда добавляет к указанному определению класса условие соответствия, основанное на значении типа ethertype. Значение **ethertype** указывается одним из следующих ключевых слов: **appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp** либо произвольное значение EtherType в диапазоне 0x06000xFFFF.

Формат match ethertype {keyword | custom 0x0600-0xFFFF}

Режим Class-Map Config

match any

Эта команда добавляет к указанному определению класса условие соответствия, при котором все пакеты считаются принадлежащими классу.

По умолчанию нет

Формат match any

Режим Class-Map Config

match class-map

Эта команда добавляет к указанному определению класса набор условий соответствия, определенных для другого класса. **r1efclassname –** это имя существующего класса DiffServ, на условия соответствия которого ссылается указанное определение класса.

По умолчанию нет

Формат Match class-map refclassname

Режим Class-Map Config

ПРИМЕЧАНИЕ:

- Параметры **refclassname** и **class-map-name** – не могут быть одинаковыми.
- Класс может ссылаться только на один класс.
- Системой блокируются любые попытки удалить класс **refclassname**, пока на класс по-прежнему ссылается любой класс **classmap-name**.
- Комбинированные критерии соответствия **class-map-name** и **refclassname** должны быть разрешенной комбинацией, для данных типов класса.
- Любые последующие изменения критериев соответствия класса **refclassname** должны соответствовать этому принципу, в противном случае попытка изменения не удается.
- Общее количество правил класса, образованных цепочкой полноценных базовых классов (включая как предшественники, так и классы-преемники), не должно

превышать максимальное для данной платформы количество. В некоторых случаях каждое удаление ссылки на другой класс уменьшает максимальное количество доступных правил в определении класса на единицу.

no match class-map

Эта команда удаляет из указанного определения класса набор условий соответствия, определенных другим классом. *r1efclassname* – это имя существующего класса DiffServ, на условия соответствия которого ссылается указанное определение класса.

Формат no match class-map *refclassname*

Режим Class-Map Config

match cos

Эта команда добавляет в указанное определение класса условие соответствия для значения Class of Service (единственный тег в пакете с одним тегом, либо первый или внешний тег 802.1Q пакета с двумя тегами). Диапазон значений: 0 – 7.

По умолчанию нет

Формат match cos 0-7

Режим Class-Map Config

match secondary-cos

Эта команда добавляет в указанное определение класса условие соответствия для вторичного значения Class of Service (внутренний тег 802.1Q пакета с двойным тегом VLAN). Диапазон значений: 0 – 7.

По умолчанию нет

Формат match secondary-cos 0-7

Режим Class-Map Config

match destination-address mac

Эта команда добавляет к указанному определению класса условие соответствия, основанное на MAC-адресе назначения пакета. Параметр **macaddr** – это любой MAC-адрес уровня 2, в формате шести двузначных шестнадцатеричных чисел, разделенных двоеточиями (например, 00:11:22:dd:ee:ff). Параметр **macmask –** это битовая маска уровня 2, (последовательность одинаковых бит не требуется), в формате шести двузначных шестнадцатеричных чисел, разделенных двоеточиями (например, ff:07:23:ff:fe:dc).

По умолчанию нет

Формат match destination-address mac *macaddr macmask*

Режим Class-Map Config

match dstip

Эта команда добавляет к указанному определению класса условие соответствия, основанное на IP-адресе назначения пакета. Параметр *ipaddr* определяет IP-адрес.

Параметр **ipmask** определяет битовую маску IP-адреса. Её значение должно состоять из последовательного множества битов 1.

По умолчанию нет

Формат match dstip ipaddr ipmask

Режим Class-Map Config

match dstl4port

Эта команда добавляет к указанному определению класса условие соответствия на основе L4 порта назначения пакета, с указанием номера порта или ключевого слова для его обозначения.

Параметр **portkey** - одно из поддерживаемых ключевых слов для стандартных портов, которые можно использовать в условии соответствия вместо номера порта. Поддерживаемые значения **portkey** на данный момент: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Каждый из них преобразуется в соответствующий номер порта. Чтобы указать условие соответствия с использованием числовой нотации, требуется один L4 номер порта. Номер порта может быть целым числом от 0 до 65535.

По умолчанию нет

Формат match dstl4port {*portkey* | *0-65535*}

Режим Class-Map Config

match ip dscp

Эта команда добавляет к указанному определению класса условие соответствия на основе поля IP DiffServ Code Point (DSCP) в пакете, который определяется как старший бит октета Service Type в заголовке IP (два младших бита не проверяются).

Значение **dscpval** указывается либо как целое число от 0 до 63, либо символически, через одно из следующих ключевых слов: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

ПРИМЕЧАНИЕ: Условия ip dscp, ip priority и ip tos соответствуют альтернативным способам задания критерия соответствия для одного и того же поля Service Type в заголовке IP, но в разных форматах.

По умолчанию нет

Формат match ip dscp dscpval

Режим Class-Map Config

match ip precedence

Эта команда добавляет к указанному определению класса условие соответствия на основе поля IP Precedence в пакете, который определяется как три старших бита октета Service Type в заголовке IP (пять младших битов не проверяются). Значение Precedence может быть целым числом от 0 до 7.

ПРИМЕЧАНИЕ: Условия ip dscp, ip priority и ip tos соответствуют альтернативным способам задания критерия соответствия для одного и того же поля Service Type в заголовке IP, но в разных форматах.

По умолчанию нет

Формат match ip precedence 0-7

Режим Class-Map Config

match ip tos

Эта команда добавляет к указанному определению класса условие соответствия на основе поля IP TOS пакете, который определяется как все восемь бит октета Service Type в заголовке IP. Значение **tosbits –** двузначное шестнадцатиричное число от 00 до FF. Значение **tosmask** – двузначное шестнадцатиричное число от 00 до FF. Параметр **tosmask** определяет позиции битов в **tosbits**, которые используются для сравнения с полем IP TOS в пакете. Например, чтобы проверить значение IP TOS, имеющее настроенные биты 7 и 5, а также пустой бит 1, и бит 7 является наиболее значительным, используйте значение **tosbits** - a0 (hex), и значение **tosmask** - a2 (hex).

ПРИМЕЧАНИЕ: Условия ip dscp, ip priority и ip tos соответствуют альтернативным способам задания критерия соответствия для одного и того же поля Service Type в заголовке IP, но в разных форматах.

ПРИМЕЧАНИЕ: Эта версия - своего рода «свободная форма» спецификации соответствия IP DSCP / Precedence / TOS - дает пользователю полный контроль при указании битов поля IP Service Type.

По умолчанию нет

Формат match ip tos tosbits tosmask

Режим Class-Map Config

match protocol

Эта команда добавляет к указанному определению класса условие соответствия на основе значения поля IP Protocol пакета, с указанием номера порта или ключевого слова для его обозначения.

Параметр **protocol-name** - одно из поддерживаемых ключевых слов, которые можно использовать для обозначения протокола. В настоящее время поддерживаются следующие значения: **icmp, igmp, ip, tcp, udp**. Значение *ip* соответствует всему набору протоколов.

Чтобы указать условие соответствия в числовом виде, используйте номер протокола, который является стандартным значением, назначенным IANA, и интерпретируется как целое число от 0 до 255.

ПРИМЕЧАНИЕ: Эта команда не проверяет значение номера протокола не из текущего списка, определенного IANA.

По умолчанию нет

Формат match protocol {*protocol-name* | *0-255*}

Режим Class-Map Config

match source-address mac

Эта команда добавляет к указанному определению класса условие соответствия, основанное на MAC-адресе источника пакета. Параметр **address** – это любой MAC-адрес уровня 2, в формате шести двузначных шестнадцатеричных чисел, разделенных

двоеточиями (например, 00:11:22:dd:ee:ff). Параметр **macmask** – это битовая маска уровня 2, (последовательность одинаковых бит не требуется), в формате шести двузначных шестнадцатеричных чисел, разделенных двоеточиями (например, ff:07:23:ff:fe:dc).

По умолчанию нет

Формат match source-address mac *address macmask*

Режим Class-Map Config

match srcip

Эта команда добавляет к указанному определению класса условие соответствия, основанное на IP-адресе источника пакета. Параметр **ipaddr** определяет IP-адрес. Параметр **ipmask** определяет битовую маску IP-адреса. Её значение должно состоять из последовательного множества битов 1.

По умолчанию нет

Формат match srcip *ipaddr ipmask*

Режим Class-Map Config

match srcip6

Эта команда добавляет к указанному определению класса условие соответствия, основанное на IP-адресе источника пакета.

По умолчанию нет

Формат match srcip6 source-ipv6-prefix/prefix-length

Режим Ipv6-Class-Map Config

match srcl4port

Эта команда добавляет к указанному определению класса условие соответствия на основе L4 порта источника пакета, с указанием номера порта или ключевого слова для его обозначения. Параметр **portkey** – одно из поддерживаемых ключевых слов для стандартных портов, которые можно использовать в условии соответствия вместо номера порта. Ключевые слова перечислены ниже. Поддерживаемые значения **portkey** на данный момент: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Каждое ключевое слово преобразуется в цифровое значение, используемое как в качестве начала диапазона портов, так и в качестве конца этого диапазона.

Чтобы указать условие соответствия в числовом виде, требуется один номер L4 порта. Номер порта может быть целым числом от 0 до 65535.

По умолчанию нет

Формат match srcl4port {portkey | 0-65535}

Режим Class-Map Config

match vlan

Эта команда добавляет в указанное определение класса соответствие условию для значения поля идентификатора VLAN (единственный тег в пакете с одним тегом, либо

первый или внешний тег 802.1Q пакета с двойным тегом). Значение VLAN ID может быть целым числом от 0 до 4094.

По умолчанию нет

Формат match vlan 0-4094

Режим Class-Map Config

`match secondary-vlan`

Эта команда добавляет в указанное определение класса соответствие условию для значения поля идентификатора Secondary VLAN уровня 2 (внутренний тег 802.1Q пакета с двойным тегом). Значение Secondary VLAN ID может быть целым числом от 0 до 4094.

По умолчанию нет

Формат match secondary-vlan 0-4094

Режим Class-Map Config

10.4. Команды политик DiffServ

Команды политики DiffServ используются для выполнения действий с трафиком, таких как маркировка и контроль, для применения к классам трафика.

Используйте команды политики, чтобы связать определяемый вами класс трафика с одним или несколькими атрибутами политики QoS. Назначьте интерфейсу связь «класс-политика» для формирования сервиса. При создании политики укажите ее имя.

Каждый класс трафика определяет конкретное действие с пакетами, соответствующими определению класса. Несколько классов трафика могут быть связаны с одной политикой. Когда пакет удовлетворяет условиям более чем одного класса, предпочтение действия основывается на порядке добавления классов в политику. Первый добавленный класс имеет высший приоритет.

Данный набор команд отвечает за создание/удаление политик, добавление/удаления классов и отдельных атрибутов политик.

ПРИМЕЧАНИЕ: Единственный способ удалить отдельный атрибут политики из экземпляра ее класса - удалить экземпляр класса и добавить его в политику заново. Значения, связанные с существующим атрибутом политики, могут быть изменены без удаления экземпляра класса.

Корневая команда: `policy-map`.

`assign-queue`

Данная команда назначает идентификатор очереди, к которому привязан ассоциируемый поток трафика. Параметр *queueid* представляет собой целое число от 0 до n-1, где n - количество выходных очередей, поддерживаемых устройством.

Формат assign-queue queueid

Режим Policy-Class-Map Config

Несовместимость Drop

drop

Данная команда указывает, что все пакеты для связанного потока трафика должны быть отброшены на входе.

Формат drop

Режим Policy-Class-Map Config

Несовместимость Assign Queue, Mark (все формы), Mirror, Police, Redirect

mirror

Данная команда указывает, что все входящие пакеты для связанного потока трафика должны быть скопированы на определенный выходной интерфейс.

Формат mirror unit/slot/port

Режим Policy-Class-Map Config

Несовместимость Drop, Redirect

redirect

Данная команда указывает, что все входящие пакеты для связанного потока трафика должны быть перенаправлены на определенный выходной интерфейс.

Формат redirect unit/slot/port

Режим Policy-Class-Map Config

Несовместимость Drop, Mirror

conform-color

Используйте эту команду, чтобы включить управление траффиком по цветам и определить карту соответствия классов цветам. Используется вместе с командой police, которая указывает поля для соответствия уровню. Параметр **class-map-name** – имя существующего класса DiffServ.

ПРИМЕЧАНИЕ: Эта команда может использоваться только после указания команды police для экземпляра класс-политика.

Формат conform-color class-map-name

Режим Policy-Class-Map Config

class

Данная команда создает экземпляр определения класса в указанной политике с целью определения класса трафика для обработки с помощью последующих инструкций политики. Параметр **classname** – имя существующего класса DiffServ.

ПРИМЕЧАНИЕ: В результате выполнения этой команды указанная политика создает ссылку на определение класса.

ПРИМЕЧАНИЕ: При успешном выполнении данной команды режим CLI изменяется на Policy-Class-Map Config.

Формат class classname

Режим Policy-Map Config

no class

Данная команда удаляет экземпляр определенного класса и определенное для него действие из указанной политики. Параметр **classname** – имя существующего класса DiffServ.

ПРИМЕЧАНИЕ: Данная команда удаляет ссылку на определение класса для указанной политики.

Формат no class classname

Режим Policy-Map Config

mark cos

Данная команда маркирует все пакеты для связанного потока трафика указанным значением Class of Service (CoS) в поле приоритета заголовка 802.1p (тег в пакете с одним тегом или первый либо внешний тег 802.1Q пакета с двойным тегом). Если пакет не содержит данного заголовка, он добавляется. Значение CoS может быть целым числом от 0 до 7.

По умолчанию 1

Формат mark-cos 0-7

Режим Policy-Class-Map Config

Несовместимость Drop, Mark IP DSCP, IP Precedence, Police

mark cos-as-sec-cos

Эта команда маркирует биты приоритета внешнего тега VLAN для всех пакетов в соответствии с приоритетом внутреннего тега VLAN, указывая CoS как вторичный CoS. Иными словами, CoS внутреннего тега VLAN копируется как CoS внешнего тега VLAN.

Формат mark-cos-as-sec-cos

Режим Policy-Class-Map Config

Несовместимость Drop, Mark IP DSCP, IP Precedence, Police

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(switch) (Config-policy-classmap)#mark cos-as-sec-cos
```

mark ip-dscp

Данная команда маркирует все пакеты для соответствующего потока трафика указанным значением IP DSCP.

Значение *dscpval* указывается либо как целое число от 0 до 63, либо как одно из следующих ключевых слов: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

Формат mark ip-dscp *dscpval*

Режим Policy-Class-Map Config

Несовместимость Drop, Mark CoS, Mark IP Precedence, Police

mark ip-precedence

Данная команда маркирует все пакеты для соответствующего потока трафика указанным значением IP Precedence. Значение IP Precedence может быть целым числом от 0 до 7.

Формат	mark ip-precedence *0-7*
Режим	Policy-Class-Map Config
Несовместимость	Drop, Mark CoS, Mark IP Precedence, Police
Тип политики	In

police-simple

Эта команда используется для определения стиля контроля обработки трафика для указанного класса. Простая форма команды **police** использует одну скорость передачи данных и размера превышения (burst size), что приводит к двум результатам: conform (соответствие) и violate (несоответствие). При соответствии скорость передачи данных указывается в килобитах в секунду (Кбит/с) и является целым числом от 1 до 4294967295. Размер превышения при соответствии указывается в килобайтах (КБ) и является целым числом от 1 до 128.

Для каждого результата возможны только следующие действия: drop, set-cos-as-sec-cos, set-cos-transmit, set-sec-costransmit, set-dscp-transmit, set-prec-transmit либо transmit. В простой форме команды **police** действиями по умолчанию являются: transmit (передача) при соответствии и drop (отклонение) при несоответствии. Эти действия могут быть настроены с помощью этой же команды после настройки стиля.

Для set-dscp-transmit значение **dscpval** указывается либо как целое число от 0 до 63, либо как одно из следующих ключевых слов: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

Для set-prec-transmit значение IP Precedence указывается либо как целое число от 0 до 7.

Для set-cos-transmit значение 802.1p priority указывается либо как целое число от 0 до 7.

Формат	police-simple 1-4294967295 1-128 conform-action {drop | set-sec-cos-transmit 07 | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit} violate-action {drop | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit}
Режим	Policy-Class-Map Config
Несовместимость	Drop, Mark (all forms)

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(switch) (Config-policy-classmap)#police-simple 1 128 conform-action transmit violate-action drop
```

police-single-rate

Эта команда является формой одной скорости (single-rate) команды **police** и используется для определения стиля контроля обработки трафика для указанного класса. Для каждого результата возможны только следующие действия: drop, set-cos-as-sec-cost, set-costransmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit либо transmit. В форме single-rate команды **police** действиями по умолчанию являются: transmit (отправка) при соответствии, drop (отклонение) при несоответствии и при превышении (exceed). Эти действия могут быть настроены с помощью этой же команды после настройки стиля.

Формат police-single-rate 1-4294967295 1-128 1-128 conform-action {drop | set-prectransmit 0-7 | set-dscp-transmit 0-63 | transmit} exceed-action {drop | set-prectransmit 0-7 | set-dscp-transmit 0-63 | transmit} violate-action {drop | setprec-transmit 0-7 | set-dscp-transmit 0-63 | transmit}

Режим Policy-Class-Map Config

police-two-rate

Эта команда является формой двух скоростей (two-rate) команды **police** и используется для определения стиля контроля обработки трафика для указанного класса. Для каждого результата возможны только следующие действия: drop, set-cos-as-sec-cos, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit либо transmit. В форме two-rate команды **police** действиями по умолчанию являются: transmit (отправка) при соответствии, drop (отклонение) при несоответствии и при превышении (exceed). Эти действия могут быть настроены с помощью этой же команды после настройки стиля.

Формат police-two-rate 1-4294967295 1-128 1-4294967295 1-128 conform-action {drop | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit} exceed-action {drop | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit} violate-action {drop | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit}

Режим Policy-Class-Map Config

policy-map

Данная команда создает новую политику DiffServ. Параметр **policyname** – это строка из букв и цифр длиной от 1 до 31 символа (чувствительно к регистру), которая является уникальным идентификатором политики. Тип политики, относящийся к входящему трафику, указывается параметром in. Тип, относящийся к исходящему трафику, соответственно, указывается параметром out.

ПРИМЕЧАНИЕ: При успешном выполнении данной команды режим CLI изменяется на Policy-Map Config.

Формат policy-map policyname {in|out}

Режим Global Config

no policy-map

Данная команда удаляет существующую политику DiffServ. Параметр **policyname** – имя существующей политики DiffServ. Команда может быть выполнена в любое время. Если на указанную политику в данный момент ссылаются одно или несколько служб присоединенных на интерфейсы, то попытка удаления не удается.

Формат no policy-map policyname

Режим Global Config

policy-map rename

Данная команда переименовывает политику DiffServ. Параметр **policyname** – имя существующей политики DiffServ. Параметр **newpolicyname** – это строка из букв и цифр длиной от 1 до 31 символа (чувствительно к регистру), которая является уникальным идентификатором политики.

Формат policy-map rename *policyname newpolicyname*

Режим Global Config

10.5. Команды служб DiffServ

Команды служб DiffServ используются для назначения политики управления трафика DiffServ для входного интерфейса, указанной ранее с помощью команд политик.

Команды служб присоединяют определенную политику к направленному интерфейсу. Входящему интерфейсу можно назначить только одну политику. Для исходящего направления DiffServ не используется.

Данный набор команд состоит из добавления и удаления служб.

Корневая команда: **service-policy**.

service-policy

Эта команда присоединяет политику к интерфейсу во входящем направлении, указанному параметром **in**, либо к интерфейсу в выходящем направлении, указанному, соответственно, параметром **out**. Параметр **policyname** – имя существующей политики DiffServ. В результате выполнения этой команды служба создает ссылку на политику.

ПРИМЕЧАНИЕ: Эта команда включает DiffServ на интерфейсе в входящем направлении. Для DiffServ не существует отдельного режима команд.

ПРИМЕЧАНИЕ: Эта команда завершается с ошибкой, если какие-либо атрибуты в определении политики превышают возможности интерфейса. После успешной привязки политики к интерфейсу любая попытка изменить определение политики, не соответствующая возможностям интерфейса, приводит к сбою попытки изменения политики.

Формат service-policy {in|out} *policymapname*

Режимы Global Config

Interface Config

ПРИМЕЧАНИЕ: К каждому интерфейсу может быть привязана только одна политика.

no service-policy

Эта команда отменяет привязку политики к интерфейсу во входящем направлении, указанному параметром **in**, либо к интерфейсу в исходящем направлении, указанному, соответственно, параметром **out**. Параметр **policyname** – имя существующей политики DiffServ.

ПРИМЕЧАНИЕ: В результате выполнения этой команды служба удаляет ссылку на политику. Эта команда отключает DiffServ на интерфейсе в входящем или исходящем направлении.

Для DiffServ не существует отдельного режима команд.

Формат no service-policy {in|out} policymapname

Режимы Global Config

Interface Config

10.6. Команды просмотра DiffServ

Команды просмотра DiffServ используются для отображения информации о конфигурации и состоянии классов, политик и служб. Информация DiffServ может выводиться как в сокращенном, так и в детальном форматах. Информация о состоянии показывается только в случае включенного административного режима DiffServ.

show class-map

Данная команда отображает всю информацию о конфигурации указанного класса. Параметр **class-name** – имя существующего класса DiffServ.

Формат show class-map class-name

Режимы Privileged EXEC

User EXEC

При указании class-name отображаются следующие поля:

Термин	Значение
Class Name	Имя данного класса.
Class Type	all - каждый определенный для класса критерий соответствия оценивается одновременно, и каждый должен быть истинным, чтобы подтвердить соответствие классу.
Class Layer3 Protocol	Протокол класса уровня 3 OSI. Возможные значения: IPv4.
Match Criteria	Критерии соответствия. Эти поля отображаются только в том случае, если критерии настроены. Некоторые критерии не поддерживаются некоторыми платформами. Отображаются в том порядке, в котором были введены пользователем. Поля оцениваются в соответствии с типом класса. Возможные критерии соответствия: Destination IP Address, Destination Layer 4 Port, Destination MAC Address, Ethertype, Source MAC Address, VLAN, Class of Service, Every, IP DSCP, IP Precedence, IP TOS, Protocol Keyword, Reference Class, Source IP Address и Source Layer 4 Port.
Values	Значения критериев соответствия.

Если не указано имя класса (Class Name), эта команда отображает список всех заданных классов DiffServ. Отображаются следующие поля:

Термин	Значение
Class Name	Имя данного класса. (Обратите внимание, что порядок отображения классов может отличаться от порядка их создания).

Термин	Значение
Class Type	all - каждый определенный для класса критерий соответствия оценивается одновременно, и каждый должен быть истинным, чтобы подтвердить соответствие классу.
Ref Class Name	Имя существующего класса DiffServ, на критерии соответствия которого ссылается определение указанного класса.

show diffserv

Данная команда отображает глобальную информацию статуса DiffServ, которая включает в себя текущую настройку административного режима, а также текущее и максимальное количество строк в каждой из основных таблиц MIB DiffServ. Дополнительные параметры для этой команды не предусмотрены.

Формат show diffserv

Режимы Privileged EXEC

User EXEC

Термин	Значение
DiffServ Admin mode	Текущее значение административного режима DiffServ.
Class Table Size Current/Max	Текущее и максимальное количество записей (строк) в таблице классов.
Class Rule Table Size Current/Max	Текущее и максимальное количество записей (строк) в таблице правил классов.
Policy Table Size Current/Max	Текущее и максимальное количество записей (строк) в таблице политик.
Policy Instance Table Size Current/Max	Текущее и максимальное количество записей (строк) в таблице экземпляров политик.
Policy Instance Table Max Current/Max	Текущее и максимальное количество записей (строк) для таблицы экземпляров политик.
Policy Attribute Table Max Current/Max	Текущее и максимальное количество записей (строк) для таблицы атрибутов политик.
Service Table Size Current/Max	Текущее и максимальное количество записей (строк) в таблице служб.

show policy-map

Данная команда отображает всю информацию о конфигурации указанной политики. Параметр **policyname** – имя существующей политики DiffServ.

Формат show policy-map [policyname]

Режим Privileged EXEC

При указании имени политики отображаются следующие поля:

Термин	Значение
Policy Name	Имя данной политики.
Policy Type	Тип политики (данная платформа поддерживает только определение входящих политик).
Class Members	Классы - члены указанной политики.

Следующая информация повторяется для каждого класса, связанного с данной политикой (отображаются только настроенные атрибуты):

Термин	Значение
Assign Queue	Направляет поток трафика в указанную очередь QoS. Это позволяет механизму классификации трафика определять, какая из аппаратных очередей должна использоваться для обработки пакетов, принадлежащих к указанному классу.
Class Name	Имя данного класса.
Committed Burst Size (KB)	Гарантированный размер превышения, используемый в простых политиках.
Committed Rate(Kbps)	Гарантированная скорость, используемая в простых политиках.
Conform Action	Текущая настройка для действия, предпринятого в пакете в случае соответствия параметрам политик. Не отображается, если не используется.
Conform COS	Значение метки CoS, если действие в случае соответствия – set-cos-transmit.
Conform DSCP Value	Значение метки DSCP, если действие в случае соответствия – set-dscp-transmit.
Conform IP Precedence Value	Значение метки IP Precedence, если действие в случае соответствия – set-prec-transmit.

Термин	Значение
Drop	Отбрасывание пакета по получению. Это полезно для эмуляции действия списка управления доступом с использованием DiffServ, особенно когда DiffServ и ACL не могут сосуществовать на одном и том же интерфейсе.
Mark CoS	Значение CoS, заданное в заголовке 802.1p входящих пакетов. Не отображается, если не указана метка CoS.
Mark IP DSCP	Значение маркировки/перемарикировки метки, используемое в качестве DSCP для трафика, соответствующего этому классу. Не отображается, если не указано действие mark ip.
Mark IP Precedence	Значение маркировки/перемарикировки, используемое в качестве IP Precedence для трафика, соответствующего этому классу. Не отображается, если указано действие ip precedence.
Mirror	Копирует классифицированный поток трафика на указанный выходной порт (физический порт или LAG). Это может происходить в дополнение к любым действиям по маркировке или применению политик. Это также может быть указано вместе с назначением очереди QoS.
Non-Conform Action	Текущая настройка для действия, предпринятого в пакете в случае несоответствия параметрам политик. Не отображается, если не используется.
Non-Conform COS	Значение метки CoS, если действие в случае несоответствия – set-cos-transmit.
Non-Conform DSCP Value	Значение метки DSCP, если действие в случае несоответствия – set-dscp-transmit.
Non-Conform IP Precedence Value	Значение метки IP Precedence, если действие в случае несоответствия – set-prec-transmit.

Термин	Значение
Peak Rate	Гарантирует определенную скорость передачи, но также передает избыточные пакеты трафика до заданной пользователем пиковой скорости, с пониманием того, что нисходящий сетевой элемент (например, ограничитель скорости следующего перехода) может сбросить этот избыточный трафик. Трафик хранится в очереди до тех пор, пока он не будет передан или удален (для каждого типа управления глубиной очереди). Формирование пиковой скорости может быть сконфигурировано для исходящего потока передачи для класса трафика AP (хотя также может быть использовано усредненное формирование скорости).
Peak Burst Size	(PBS). Администратор может настроить PBS в качестве средства ограничения ущерба, который ускоренный трафик пересылки может нанести другому трафику Трафик, превышающий этот предел, отбрасывается.
Policing Style	Используемый стиль применения политик, если есть (simple).
Redirect	Направляет классифицированный поток трафика на указанный выходной порт (физический порт или LAG). Это может происходить в дополнение к любым действиям по маркировке или применению политик. Это также может быть указано вместе с назначением очереди QoS.

Если имя политики не указано, эта команда отображает список всех заданных политик DiffServ. Отображаются следующие поля:

Термин	Значение
Policy Name	Имя данной политики. (Обратите внимание, что порядок отображения политик может отличаться от порядка их создания).
Policy Type	Тип политики (поддерживаются только входящие).
Class Members	Список имен всех классов, связанных с данной политикой.

ПРИМЕР: Пример вывода командной строки при включенной в качестве действия политики опции mark-cos-as-sec-cos.

```
(Routing) #show policy-map p1
Policy Name.....p1
Policy Type .....In
Class Name.....c1
Mark CoS as Secondary CoS .....Yes
```

ПРИМЕР: Пример вывода командной строки, включающий действие mark-cos-as-sec-cos, используемое в команде policing (simple-police, police-single-rate, police two-rate).

```
(Routing) #show policy-map p2
Policy Name.....p2
Policy Type .....In
Class Name.....c2
Policing Style.....Police Two Rate
Committed Rate .....1
Committed Burst Size.....1
Peak Rate.....1
Peak Burst Size.....1
Conform Action .....Mark CoS as Secondary CoS
Exceed Action .....Mark CoS as Secondary CoS
Non-Conform Action.....Mark CoS as Secondary CoS
Conform Color Mode.....Blind
Exceed Color Mode.....Blind
```

show diffserv service

Данная команда отображает информацию службы политик для указанного интерфейса и направления. Параметр **unit/slot/port** указывает порт в системе.

Формат show diffserv service unit/slot/portin

Режим Privileged EXEC

Термин	Значение
DiffServ Admin Mode	Текущее значение административного режима DiffServ. Привязанная политика имеет эффект только в том случае, если DiffServ включен.
Interface	unit/slot/port
Direction	Направление трафика службы данного интерфейса.
Operational Status	Текущий статус интерфейса службы DiffServ.
Policy Name	Имя политики, привязанной к интерфейсу в указанном направлении.
Policy Details	Информация о привязанной политике, идентичное тому, которое описано для команды **show policy-map policymapname** (в данном Примере мы не приводим его для краткости).

show diffserv service brief

Эта команда отображает все интерфейсы в системе, к которым была привязана политика DiffServ. Параметр входящего направления – необязательный.

Формат show diffserv service brief [in]

Режим Privileged EXEC

Термин	Значение
DiffServ Mode	Текущее значение административного режима DiffServ. Привязанная политика активна только в том случае, если DiffServ включен.

Следующая информация повторяется для интерфейса и направления (показываются только те интерфейсы, к которым привязана политика):

Термин	Значение
Interface	unit/slot/port
Direction	Направление трафика службы данного интерфейса.
OperStatus	Текущий статус интерфейса службы DiffServ.
Policy Name	Имя политики, привязанной к интерфейсу в указанном направлении.

show policy-map interface

Данная команда отображает статистику политик для указанного интерфейса и направления. Параметр **unit/slot/port** указывает действительный интерфейс в системе. Для указания интерфейса LAG вместо **unit/slot/port** можно использовать lag **lag-intf-num**. Также для определения интефейса LAG можно использовать lag **lag-intf-num**, где **lag-intf-num** - номер порта LAG.

ПРИМЕЧАНИЕ: Команда доступна только в случае включенного административного режима DiffServ.

Формат show policy-map interface unit/slot/port {in | out}

Режим Privileged EXEC

Термин	Значение
Interface	unit/slot/port
Direction	Направление трафика службы данного интерфейса.
Operational Status	Текущий статус интерфейса службы DiffServ.

Термин	Значение
Policy Name	Имя политики, привязанной к интерфейсу в указанном направлении.

Следующая информация повторяется для каждого экземпляра класса в рамках данной политики:

Термин	Значение
Class Name	Имя данного экземпляра класса.
In Discarded Packets	Количество пакетов, отброшенных для данного экземпляра класса по причине того или иного действия DiffServ класса трафика.

show service-policy

Данная команда отображает сводную статистику политик для всех интерфейсов и направлений.

Формат show service-policy in

Режим Privileged EXEC

User EXEC

Следующая информация повторяется для каждого интерфейса и направления (показываются только те интерфейсы, к которым привязана политика):

Термин	Значение
Interface	unit/slot/port
Operational Status	Текущий статус интерфейса службы DiffServ.
Policy Name	Имя политики, привязанной к интерфейсу.

10.7. Команды MAC Access Control List

В этом разделе описаны команды, используемые для настройки списков контроля доступа на основе MAC (MAC ACL). Списки MAC ACL отвечают за то, чтобы только авторизованные пользователи имели доступ к определенным ресурсам, и блокируют любые нежелательные попытки достичь сетевых ресурсов.

К спискам MAC ACL применяются следующие правила:

- Максимальное количество ACL, которые вы можете создать, зависит от оборудования. Ограничение применяется ко всем спискам ACL, независимо от типа.
- Система поддерживает только фреймы типа Ethernet II.
- Максимальное количество правил на один ACL зависит от оборудования.

mac access-list extended

Данная команда создает MAC ACL, идентифицируемый по имени – *name*. Список состоит из полей классификации, определенных для L2 заголовка Ethernet-фрейма. Параметр *name* – это строка из букв и цифр длиной от 1 до 31 символа (чувствительно к регистру), которая является уникальным идентификатором ACL. Атрибут rate-limit настраивает гарантированную скорость и гарантированный размер превышения.

Если MAC ACL с таким именем уже существует, команда активирует режим Mac-Access-List config для обновления существующего ACL.

ПРИМЕЧАНИЕ: После успешного выполнения этой команды режим командной строки меняется на Mac-Access-List config.

Формат mac access-list extended *name*

Режим Global Config

no mac access-list extended

Данная команда удаляет из системы MAC ACL, определяемый именем *name*.

Формат no mac access-list extended *name*

Режим Global Config

mac access-list extended rename

Данная команда позволяет изменить имя списка MAC ACL. Параметр **name** – имя существующего MAC ACL. Параметр **newname** – это строка из букв и цифр длиной от 1 до 31 символа (чувствительно к регистру), которая является уникальным идентификатором MAC ACL.

Команда не выполняется в том случае, если MAC ACL с именем **newname** уже существует.

Формат mac access-list extended rename name newname

Режим Global Config

mac access-list resequence

Данная команда позволяет перенумеровать записи для указанного списка доступа MAC, с заданным значением инкрементирования, начиная с определенного порядкового номера. Команда используется для редактирования порядковых номеров правил в ACL и изменения порядка внесения записей. Эта команда не сохраняется в конфигурации запуска и не отображается в текущей конфигурации.

По умолчанию 10

Формат mac access-list resequence name starting-sequence-number increment

Режим Global Config

Параметр	Описание
starting-sequencenumber	Начальный порядковый номер. Диапазон: 1 – 2147483647. Значение по умолчанию - 10.

Параметр	Описание
increment	Инкремент. Диапазон: 1 – 2147483647. Значение по умолчанию - 10.

{deny | permit} (MAC ACL)

Данная команда создает новое правило для текущего MAC ACL. Правило может отклонять или пропускать трафик в соответствии с указанными полями классификации. Как минимум, необходимо указать значение MAC-адреса источника и назначения, каждый из которых может быть заменен ключевым словом «any», чтобы указать совпадение с любым возможным значением в этом поле. Остальные параметры команды являются необязательными, но наиболее часто используемые параметры отображаются в порядке, показанном ниже.

Формат [*sequence number*] {deny|permit} {*srcmac* | any} {*dstmac* | any} [*ethertypekey* | *0x06000xFFFF*] [vlan {eq *0-4095*}] [cos *0-7*] [[log] [time-range *time-range-name*] [assign-queue *queue-id*]] [{mirror | redirect} *unit/slot/port*][rate-limit *rate burst-size*]

Режим Mac-Access-List Config

ПРИМЕЧАНИЕ: Неявно выраженное правило deny all всегда завершает список ACL.

«Sequence-number» указывает порядковый номер правила ACL. Данный номер может быть как назначен пользователем, так и сгенерирован устройством.

Если для правила не указан порядковый номер, используется номер на 10 больший, чем последний порядковый номер в ACL. Само правило при этом помещается в конец списка. Если это первое правило ACL в данном списке, ему назначается порядковый номер 10. Если сгенерированный порядковый номер превышает максимальное значение, создание правила ACL завершается с ошибкой. Нельзя создать правило, которое дублирует уже существующее. Также правило не может быть настроено с порядковым номером, уже используемым для другого правила.

Например, если пользователь добавляет в ACL новое правило без указания порядкового номера, оно помещается в конец списка. Изменяя порядковый номер правило, пользователь может изменить позицию этого правила в ACL.

Ethertype может быть указан как ключевым словом, так и четырехзначным шестнадцатеричным значением от 0x0600-0xFFFF. Поддерживаемые в настоящий момент значения *ethertypekey*: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp. Каждый из них преобразуется в соответствующее значение Ethertype.

Ключевые слова Ethertype и 4-значные шестнадцатеричные значения

Ключевое слово Ethertype	Значение
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5

Ключевое слово Ethertype	Значение
ipv4	0x0800
ipv6	0x86DD
ipx	0x8037
mplsmcast	0x8848
mplsucast	0x8847
netbios	0x8191
novell	0x8137, 0x8138
pppoe	0x8863, 0x8864
rarp	0x8035

Параметры **vlan** и **cos** относятся к полям VLAN ID и пользовательского приоритета 802.1p тега VLAN соответственно. Для пакетов, содержащих двойной тег VLAN, это первый (или внешний) тег.

Параметр time-range позволяет налагать ограничение по времени на правило ACL MAC, согласно параметру time-range-name. Если временной диапазон с указанным именем не существует, и ACL MAC, содержащий это правило, применяется к интерфейсу или привязан к VLAN, тогда правило ACL применяется немедленно. Если временной диапазон с указанным именем существует, и ACL MAC, содержащий это правило, применяется к интерфейсу или привязан к VLAN, тогда правило ACL применяется по наступлению начала указанного диапазона времени. Правило ACL удаляется по истечению временного диапазона с указанным именем. Информацию о настройке диапазонов времени см. “Команды диапазона времени для Time-Based ACL”.

Параметр **assign-queue** позволяет указать определенную аппаратную очередь для обработки трафика, соответствующего этому правилу. Допустимое значение **queue-id** равно 0-(n-1), где n - количество настраиваемых пользователем очередей, доступных для конкретной аппаратной платформы. Параметр **assign-queue** применяется только для правила **permit**.

Параметр **mirror** позволяет скопировать трафик, соответствующий этому правилу, на указанный **unit/slot/port**, в то время как параметр «**redirect**» позволяет перенаправить трафик, соответствующий этому правилу, на **unit/slot/port**. Параметры **assign-queue** и **redirect** применяется только для правила **permit**.

ПРИМЕЧАНИЕ: Особая форма команды **{deny | permit} any any** используется для отбора всех пакетов уровня 2 Ethernet и является эквивалентом правила “**match every**” списка IP ACL.

Дополнительный атрибут команды **permit**, **rate-limit**, позволяет разрешить только допустимую скорость передачи данных, указанную в Кбит/с, и размер превышения (в КБ).

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)#mac access-list extended mac1
```

```
(Routing) (Config-mac-access-list)#permit 00:00:00:00:aa:bb ff:ff:ff:ff:00:00 any rate-limit 32 16
(Routing) (Config-mac-access-list)#exit
```

no sequence-number

Данная команда позволяет удалить правило ACL с указанным номером sequence number из ACL.

Формат no sequence-number

Режим MAC-Access-List Config

mac access-group

Данная команда либо присоединяет определенный список управления доступом к MAC (ACL), идентифицированный по имени, интерфейсу или диапазону интерфейсов; либо связывает его с идентификатором VLAN в заданном направлении. Параметр *name* – имя существующего MAC ACL.

Необязательный параметр «sequence» указывает порядок этого списка MAC ACL по отношению к другим MAC ACL, уже назначенных этому интерфейсу и направлению. Чем ниже значение, тем выше приоритет. Если указанный параметр «sequence» уже используется для этого интерфейса и направления, указанный MAC ACL заменяет текущий MAC ACL, используя этот порядковый номер. Если «sequence» для этой команды не указан, используется значение приоритета большее, чем самое большое из уже используемых для этого интерфейса и направления.

Эта команда, запущенная в режиме «Interface Config», распространяет свое действие на один интерфейс, а в режиме «Global Config» – на все интерфейсы. Ключевое слово «VLAN» действует только в режиме «Global Config».

Для применения MAC ACL на порте CPU указывается параметр control-plane (необязательно). Пакеты управления, такие как BPDU, также отбрасываются из-за неявного правила deny all, добавленного в конец списка. Для нейтрализации этого эффекта в конец списка необходимо добавить правила разрешения (permit).

ПРИМЕЧАНИЕ: Ключевое слово «control-plane» доступно только в режиме «Global Config».

ПРИМЕЧАНИЕ: Опция *out* может быть недоступной на некоторых платформах.

Формат mac access-group name {{control-plane|in|out} | vlan vlan-id {in|out}} [sequence 1–4294967295]

Режимы Global Config

Interface Config

Параметр	Описание
name	Имя ACL.
sequence	Значение приоритета этого списка MAC ACL по отношению к другим MAC ACL, уже назначенных этому интерфейсу и направлению. Диапазон - от 1 до 4294967295.

Параметр	Описание
vlan-id	VLAN ID, связанный с определенным IP ACL в заданном направлении.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing)(Config)#mac access-group mac1 control-plane
```

no mac access-group

Данная команда удаляет MAC ACL, определяемый именем *name*, из указанного интерфейса и указанного направления.

Формат no mac access-group name {{control-plane|in|out} | vlan vlan-id {in|out}}

Режимы Global Config

Interface Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing)(Config)#no mac access-group mac1 control-plane
```

remark

Данная команда добавляет новый комментарий к правилу ACL.

Ключевое слово «remark» добавляет комментарий к записям правил, принадлежащим к спискам ACL следующих типов: IPv4, IPv6, MAC. Максимальное количество комментариев, доступное для правила ACL – 10. Общая длина комментария не может превышать 100 символов. Комментарий может содержать символы в следующих диапазонах: A-Z, a-z и 0-9, а также специальные символы, такие как пробел, тире и знак подчеркивания. Комментарии связываются с правилом ACL, которое создается сразу после создания комментария. При удалении правила ACL связанные комментарии также удаляются. Комментарии показываются только в выводе команды show running-config и не отображаются в выводе команды **show ip access-lists**.

Комментарии могут быть добавлены только перед созданием правила. Если пользователь создает до 10 комментариев, каждый из них связывается со следующим созданным правилом.

По умолчанию Нет

Формат remark comment

Режим IPv4-Access-List Config

IPv6-Access-List-Config

MAC-Access-List Config

no remark

Данная команда удаляет комментарий из ACL.

Комментарий удаляется при нахождении первого совпадения в ACL. Повторное выполнение этой команды с указанием этого же комментария удаляет его из следующего правила ACL, у которого есть связанный с ним комментарий (если есть какое-либо

правило, настроенное с тем же комментарием). Если с данным комментарием больше не связано ни одного правила, команда возвращает сообщение об ошибке.

Если нет такого комментария, связанного с каким-либо правилом, и такой комментарий относится к числу не связанных, он удаляется.

По умолчанию Нет

Формат no remark comment

Режим IPv4-Access-List Config

IPv6-Access-List-Config

MAC-Access-List Config

show mac access-lists

Эта команда отображает список MAC ACL и все правила, определенные для него. Параметр *[name]* идентифицирует конкретный MAC ACL. Атрибут **rate-limit** отображает значения гарантированных скорости и burst size.

ПРИМЕЧАНИЕ: Вывод команды зависит от критериев соответствия, установленных в правилах ACL.

Формат show mac access-lists [*name*]

Режим Privileged EXEC

Термин	Значение
Rule Number	Порядковый номер (идентификатор) правила, определенный в пределах MAC ACL.
Action	Действите, связанное с каждым правилом. Возможные значения: Permit (разрешить) и Deny (запретить).
Source MAC Address	MAC-адрес источника для этого правила.
Source MAC Mask	MAC-маска источника для этого правила.
Committed Rate	Гарантированная скорость, определяемая атрибутом «rate-limit».
Committed Burst Size	Гарантированный размер превышения, определяемый атрибутом «rate-limit».
Destination MAC Address	MAC-адрес назначения для этого правила.
Ethertype	Ключевое слово Ethertype или пользовательское значения для данного правила.
VLAN ID	Идентификатор (либо диапазон) VLAN для этого правила.

Термин	Значение
COS	Значение COS (802.1p) для данного правила.
Log	Отображается при включении журналирования для данного правила.
Assign Queue	Идентификатор очереди, куда назначаются пакеты, соответствующие критериям данного правила.
Redirect Interface	*unit/slot/port*, на который пересылаются пакеты, соответствующие критериям данного правила.
Time Range Name	Имя временного диапазона, если правило MAC ACL содержит ссылки на него.
Rule Status	Состояние данного правила MAC ACL. Возможные значения: Active (активно) и Inactive (неактивно).

ПРИМЕР: Пример вывода командной строки для данной команды.

```
(Routing) #show mac access-lists mac1
ACL Name: mac1
Outbound Interface(s): control-plane
Sequence Number: 10
Action .....permit
Source MAC Address.....00:00:00:00:AA:BB
Source MAC Mask .....FF:FF:FF:FF:00:00
Committed Rate .....32
Committed Burst Size.....16
Sequence Number: 25
Action .....permit
Source MAC Address.....00:00:00:00:AA:BB
Source MAC Mask .....FF:FF:FF:FF:00:00
Destination MAC Address .....01:80:C2:00:00:00
Destination MAC Mask.....00:00:00:FF:FF:FF
Ethertype .....ipv6
VLAN.....36
CoS Value.....7
Assign Queue .....4
Redirect Interface.....0/34
Committed Rate .....32
Committed Burst Size.....16
```

10.8. Команды IP Access Control List

В этом разделе описаны команды, используемые для настройки списков контроля доступа IP (IP ACL). Списки IP ACL отвечают за то, чтобы только авторизованные пользователи имели доступ к определенным ресурсам, и блокируют любые нежелательные попытки достичь сетевых ресурсов.

К спискам IP ACL применяются следующие правила:

- ПО коммутатора не подерживает конфигурацию IP ACL для фрагментов IP-пакетов.
- Максимальное количество ACL, которые вы можете создать, зависит от оборудования. Ограничение применяется ко всем спискам ACL, независимо от типа.
- Максимальное количество правил на один ACL зависит от оборудования.
- Обратная маска для ACL работает иначе, чем маски подсети. Обратная маска представляет собой инверсию маски подсети. В случае с маской подсети, маска имеет единицы (1) в битовых позициях, которые используются для сетевого адреса, и имеет нули (0) для битовых позиций, которые не используются. Обратная маска, напротив, имеет (0) в битовой позиции, которая должна быть проверена. 1 в битовой позиции маски ACL указывает, что соответствующий бит можно игнорировать.

access-list

Данная команда создает список контроля доступа IP (IP ACL), который идентифицируется по номеру, в диапазоне: 1-99 – для стандартных списков ACL, 100-199 – для расширенных списков ACL. Таблица ниже описывает параметры для команды access-list.

Стандартный список IP ACL:

Формат access-list 1-99 {remark comment} | {[sequence-number]} {deny | permit} {every | srcip srcmask} [log] [time-range time-range-name][assign-queue queue-id] [{mirror | redirect} unit/slot/port]

Режим Global Config

Расширенный список IP ACL:

Формат access-list *100-199* {remark *comment*} | {[*sequence-number*]} {deny | permit} {every | {{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp |

0-255} {srcip srcmask|any|host srcip}[range {portkey|startport} {portkey|endport}

{eq|neq||lt|gt} {*portkey*|*0-65535*}{*dstip dstmask*|any|host *dstip*}[{range

{portkey|startport} {portkey|endport} | {eq | neq | lt | gt} {portkey | 0-65535}]

[flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [icmp-type *icmp-type* [icmp-code *icmp-code*] | icmp-message *icmpmessage*] [igmp-type *igmp-type*] [fragments] [precedence *precedence* | tos *tos* [tosmask]| dscp *dscp*]}} [time-range *time-range-name*] [log] [assign-queue *queue-id*] [{mirror| redirect} *unit/slot/port*] [rate-limit *rate burst-size*]

Режим Global Config

ПРИМЕЧАНИЕ: Расширенные списки IPv4 ACL имеют следующие ограничения для исходящих ACL:

Отбор на диапазоне портов не поддерживается.

Команда rate-limit не поддерживается.

Параметры команды ACL

Параметр	Описание
remark *comment*	Используйте ключевое слово «remark», чтобы добавить комментарий к стандартному или расширенному IP ACL. Комментарии повышают удобство работы с ACL. Каждый комментарий может содержвать до 100 символов. Комментарий может содержать символы: A-Z, a-z и 0-9, а также специальные символы: пробел, тире и знак подчеркивания. Комментарии отображаются только в show running configuration. Для стандартного или расширенного IP ACL к одному правилу может быть добавлен только один комментарий. Пользователь может удалить только комментарии, которые не связаны с правилом. Связанные с правилом комментарии удаляются при удалении самого правила.
sequence-number	Указывает порядковый номер для правила ACL. Каждое правило получает свой номер. Данный номер может быть как назначен пользователем, так и сгенерирован устройством. Если для правила не указан порядковый номер, используется номер на 10 больший, чем последний порядковый номер в ACL. Само правило при этом помещается в конец списка. Если это первое правило ACL в данном списке, ему назначается порядковый номер 10. Если сгенерированный порядковый номер превышает максимальное значение, создание правила ACL завершается с ошибкой. Нельзя создать правило, которое дублирует уже существующее. Также правило не может быть настроено с порядковым номером, уже используемым для другого правила. Например, если пользователь добавляет в ACL новое правило без указания порядкового номера, оно помещается в конец списка. Изменяя значение sequence-number, пользователь может изменить позицию этого правила в ACL.
1-99 or *100-199*	Номера стандартного IP ACL принадлежат к диапазону 1 – 99. Номера расширенного IP ACL принадлежат к диапазону 100 – 199.

Параметр	Описание
{deny | permit}	Указывает, запрещает ли данное правило некое действие или, наоборот, разрешает
every	Соответствие каждому пакету.
{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | *0 - 255*}	Задает протокол для фильтрации расширенного правила IP ACL.
srcip srcmask|any|host scrip	Указывает IP-адрес источника и маску подсети источника в качестве критерия для соответствия правила IP ACL. Значения srcip 0.0.0.0 и srcmask 255.255.255.255 указывают на соответствие любым значениям. Указание host A.B.C.D указывает значение srcip A.B.C.D и srcmask – 0.0.0.0.
{range{portkey|startport}{portkey|endport}|{eq|neq|lt|gt} {portkey| 0-65535}]	**ПРИМЕЧАНИЕ:** Данная опция доступна только с протоколами TCP и UDP. Указывает критерий соответствия для L4 порта-источника для правила IP ACL. Вы можете указать номер порта в диапазоне 0-65535, либо указать значение portkey в виде одного из следующих ключевых слов: Для TCP: bgp, domain, echo, ftp, ftp-data, http, smtp, telnet, www, pop2, pop3. Для UDP: domain, echo, ntp, rip, snmp, tftp, time, и who. Для протоколов TCP и UDP каждое ключевое слово преобразуется в цифровое значение, используемое в качестве начала и конца диапазона портов. Если задан диапазон, правило IP ACL работает только для L4 портов, попадающих в указанный диапазон. Параметры «startport» и «endport» определяют первый и последний порты диапазона. Они могут иметь значения в диапазоне 0 – 65535. Конечный порт диапазона должен быть не меньше начального. Диапазон портов считается включительно: к нему принадлежат первый и последний порты, а также все порты между ними. При указании «eq» правило IP ACL фиксирует соответствие только для тех случаев, когда номер L4 порта совпадает с указанным портом (порт может быть указан номеров или ключевым словом).

Параметр	Описание
{range{portkey|startport}{portkey|endport}|{eq|neq|lt|gt} {portkey|0-65535}]	При указании «lt» правило IP ACL фиксирует соответствие только для тех случаев, когда номер L4 порта меньше указанного порта. По сути, это эквивалентно диапазону от 0 до <номер указанного порта – 1>. При указании «gt» правило IP ACL фиксирует соответствие только для тех случаев, когда номер L4 порта больше указанного порта. По сути, это эквивалентно диапазону от <номер указанного порта + 1> до 65535. При указании «neq» правило IP ACL фиксирует соответствие только для тех случаев, когда номер L4 порта не совпадает с указанным портом. Добавляются сразу два правила, одно из них – с диапазоном от 0 до <номер указанного порта – 1>, второе – с диапазоном от <номер указанного порта + 1> до 65535. **ПРИМЕЧАНИЕ:** Соответсвия по номерам портов применимы только к нефрагментированным пакетам и к первым фрагментам.
dstip dstmask|any|host dstip	Указывает IP-адрес назначения и маску подсети в качестве критерия соответствия правила IP ACL. Значения dstip 0.0.0.0 и dstmask 255.255.255.255 указывают на соответствие любым значениям. Указание host A.B.C.D указывает значение dstip A.B.C.D и dstmask – 0.0.0.0.
[precedence precedence | tos tos [tosmask] | dscp dscp]	Указывает TOS для правила IP ACL в зависимости от соответствия приоритета или значений DSCP, используя параметры dscp, precedence, tos/tosmask. ПРИМЕЧАНИЕ: tosmask является необязательным параметром.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	**ПРИМЕЧАНИЕ:** Данная опция доступна только с протоколом TCP. Указывает, соответствие флагам TCP в IP ACL. При указании +<tcpflagname> соответствие фиксируется в том случае, если указанный флаг <tcpflagname> установлен в заголовке TCP. При указании -<tcpflagname> соответствие фиксируется в том случае, если указанный флаг <tcpflagname> НЕ установлен в заголовке TCP. При указании «established» соответствие фиксируется в том случае, если указанные биты RST или ACK установлены в заголовке TCP. При указании опции «established» на устройство устанавливаются два правила.

Параметр	Описание
[icmp-type *icmp-type* [icmp-code *icmp-code*] | icmp-message *icmp- message*]	**ПРИМЕЧАНИЕ:** Данная опция доступна только с протоколом ICMP. Указывает условие соответствия для пакетов ICMP. При указании «icmp-type» правило IP ACL фиксирует соответствие при сообщении ICMP с указанным типом (число в диапазоне 0 – 255). При указании «icmp-code» правило IP ACL фиксирует соответствие при сообщении ICMP с указанным кодом (число в диапазоне 0 – 255). Задание «icmp-message» подразумевает, что указаны как icmp-тип, так и icmp-код. Поддерживаются следующие icmp-сообщения: echo, echo-reply, host-redirect, mobile-redirect, net-redirect, netunreachable, redirect, packet-too-big, port-unreachable, sourcequench, router-solicitation, router-advertisement, time-exceeded, ttlexceeded и unreachable.
igmp-type *igmp-type*	Данная опция доступна только с протоколом IGMP. При указании «igmp-type» правило IP ACL фиксирует соответствие сообщения IGMP указанному типу (число в диапазоне 0 – 255).
fragments	При указании этой опции правило IP ACL фиксирует соответствие для фрагментированных IP-пакетов.
[log]	Указывает, что для правила должен вестись журнал.
[time-range time-range-name]	Позволяет налагать ограничение времени на правило ACL, определяемое параметром time-range-name. Если временной диапазон с указанным именем не существует, и ACL, содержащий это правило, применяется к интерфейсу или привязан к VLAN, тогда правило ACL применяется немедленно. Если временной диапазон с указанным именем существует, и ACL, содержащий это правило, применяется к интерфейсу или привязан к VLAN, тогда правило ACL применяется по наступлению начала указанного диапазона времени. Правило ACL удаляется по истечению временного диапазона с указанным именем. Информацию о настройке диапазонов времени см. “Команды диапазона времени для ACL, контролируемого по времени” на стр. 671.
[assign-queue *queue-id*]	Задает параметр assign-queue, идентификатор очереди, которой назначаются пакеты, соответствующие этому правилу.

Параметр	Описание
[{mirror | redirect} *unit/slot/ port*]	Задает интерфейс типа «mirror» или «redirect» с указанными *unit/slot/port*, на который будут, соответственно, копироваться или пересылаться пакеты.
[rate-limit *rate burst-size*]	Указывает разрешенную скорость трафика в соответствии с настроенной скоростью в Кбит/с и размером превышения в КБ.

no access-list

Данная команда удаляет из системы IP ACL, определяемый именем **accesslistnumber**. Диапазон для **accesslistnumber**: 1-99 для стандартных ACL и 100-199 – для расширенных.

Формат no access-list accesslistnumber

Режим Global Config

ip access-list

Данная команда создает расширенный список IP Access Control List (ACL), идентифицируемый по имени (name). Список состоит из полей классификации, определенных для IP-заголовка IPv4-фрейма. Параметр name – это строка из букв и цифр длиной от 1 до 31 символа (чувствительно к регистру), которая является уникальным идентификатором ACL. Атрибут rate-limit настраивает гарантированную скорость и гарантированный размер превышения.

Если IP ACL с таким именем уже существует, команда активирует режим «IPv4-Access_List config» для обновления существующего ACL.

ПРИМЕЧАНИЕ: После успешного выполнения этой команды режим командной строки меняется на «IPv4 Access-List config».

Формат ip access-list name

Режим Global Config

no ip access-list

Данная команда удаляет из системы IP ACL, определяемый именем name.

Формат no ip access-list name

Режим Global Config

ip access-list rename

Данная команда позволяет изменить имя списка IP ACL. Параметр name – имя существующего IP ACL. Параметр newname – это строка из букв и цифр длиной от 1 до 31 символа (чувствительно к регистру), которая является уникальным идентификатором IP ACL.

Команда не выполняется в том случае, если IP ACL с именем newname уже существует.

Формат ip access-list rename name newname

Режим Global Config

ip access-list resequence

Данная команда позволяет перенумеровать записи для указанного списка доступа IP, с заданным значением инкрементирования, начиная с определенного порядкового номера. Команда используется для редактирования порядковых номеров правил в ACL и изменения порядка внесения записей. Эта команда не сохраняется в конфигурации запуска и не отображается в текущей конфигурации.

По умолчанию 10

Формат ip access-list resequence {name| id } starting-sequence-number increment

Режим Global Config

Параметр	Описание
starting-sequencenumber	Начальный порядковый номер. Диапазон: 1 – 2147483647. Значение по умолчанию - 10.
increment	Инкремент. Диапазон: 1 – 2147483647. Значение по умолчанию - 10.

{deny | permit} (IP ACL)

Данная команда создает новое правило для текущего IP ACL. Правило может отклонять или пропускать трафик в соответствии с указанными полями классификации. Как минимум, необходимо указать либо ключевое слово «every» либо протокол, адрес источника и адрес назначения. IP-адреса источника и назначения могут быть заменены ключевым словом «any», чтобы указать совпадение с любым возможным значением в этом поле. Остальные параметры команды являются необязательными, но наиболее часто используемые параметры отображаются в порядке, показанном ниже.

Формат [sequence *number*] {deny | permit} {every | {{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | *0 -255*} {srcip *srcmask* | any | host *srcip*} [{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}] {*dstip dstmask* | any | host *dstip*} [{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}] [flag [+fin | -fin] [+syn | -syn] [+rst | rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [icmp-type *icmp-type* [icmp-code icmp-code] | icmp-message icmp-message] [igmp-type igmp-type] [fragments] [precedence *precedence* | tos *tos* [*tosmask*] | dscp *dscp*]}} [time-range *time-rangename*] [log] [assign-queue *queue-id*] [{mirror | redirect} *unit/slot/port*] [rate-limit *rate burst-size*]

Режим Ipv4-Access-List Config

ПРИМЕЧАНИЕ: Неявно выраженное правило **deny all** всегда завершает список ACL.

ПРИМЕЧАНИЕ: Параметр *mirror* позволяет скопировать трафик, соответствующий этому правилу, на указанный **unit/slot/port**, в то время как параметр «redirect» позволяет перенаправить трафик, соответствующий этому правилу, на **unit/slot/port**. Параметры **assign-queue** и **redirect** применяется только для правила permit.

ПРИМЕЧАНИЕ: Для IPv4, выходные ACL не поддерживают следующее:

- Отбор на диапазоне портов не поддерживается.
- Команда rate-limit не поддерживается.

Параметр	Описание
sequence-number	«Sequence-number» указывает порядковый номер правила ACL. Данный номер может быть как назначен пользователем, так и сгенерирован устройством. Если для правила не указан порядковый номер, используется номер на 10 больший, чем последний порядковый номер в ACL. Само правило при этом помещается в конец списка. Если это первое правило ACL в данном списке, ему назначается порядковый номер 10. Если сгенерированный порядковый номер превышает максимальное значение, создание правила ACL завершается с ошибкой. Нельзя создать правило, которое дублирует уже существующее. Также правило не может быть настроено с порядковым номером, уже используемым для другого правила. Например, если пользователь добавляет в ACL новое правило без указания порядкового номера, оно помещается в конец списка. Изменяя порядковый номер правило, пользователь может изменить позицию этого правила в ACL.
{deny | permit}	Указывает, запрещает ли данное правило соответствующий трафик или, наоборот, разрешает.
Every	Соответствие каждому пакету.
{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | *0 -255*}	Указывает соответствие протокола для правила IP ACL.
srcip srcmask | any | host srcip	Указывает IP-адрес и маску подсети в качестве критерия соответствия условию правила IP ACL. Значения srcip 0.0.0.0 и srcmask 255.255.255.255 указывают на соответствие любым значениям. Указание host A.B.C.D указывает значение srcip A.B.C.D и srcmask – 0.0.0.0.

Параметр	Описание
range {portkey | startport} {portkey | endport} | {eq | neq | lt | gt} {portkey | 0-65535}]	**ПРИМЕЧАНИЕ:** Данная опция доступна только с протоколами TCP и UDP. Указывает L4- порт в качестве критерия соответствия условию правила IP ACL. Допускается использование как номера порта (в диапазоне 0 – 65535) либо ключевого слова, которое может быть одним из следующих: Для протокола TCP: bgp, domain, echo, ftp, ftp-data, http, smtp, telnet, www, pop2, pop3 Для протокола UDP: domain, echo, ntp, rip, snmp, tftp, time, who Каждое ключевое слово преобразуется системой в соответствующий номер порта. Если задан диапазон, правило IP ACL работает только для портов уровня 4, попадающих в указанный диапазон. Параметры «startport» и «endport» определяют первый и последний порты диапазона. Они могут иметь значения в диапазоне 0 – 65535. Конечный порт диапазона должен быть не меньше начального. Диапазон портов считается включительно: к нему принадлежат первый и последний порты, а также все порты между ними. При указании «eq» правило IP ACL фиксирует соответствие только для тех случаев, когда номер L4 порта совпадает с указанным портом (порт может быть указан номеров или ключевым словом). При указании «lt» правило IP ACL фиксирует соответствие только для тех случаев, когда номер L4 порта меньше указанного порта. По сути, это эквивалентно диапазону от 0 до <номер указанного порта – 1>. При указании «gt» правило IP ACL фиксирует соответствие только для тех случаев, когда номер L4 порта больше указанного порта. По сути, это эквивалентно диапазону от <номер указанного порта + 1> до 65535. При указании «neq» правило IP ACL фиксирует соответствие только для тех случаев, когда номер L4 порта не совпадает с указанным портом. Добавляются сразу два правила, одно из них – с диапазоном от 0 до <номер указанного порта – 1>, второе – с диапазоном от <номер указанного порта + 1> до 65535. **ПРИМЕЧАНИЕ:** Соответствия по номерам портов применимы только к нефрагментированным пакетам и к первым фрагментам.

Параметр	Описание
dstip dstmask | any | host dstip	Указывает IP-адрес и маску подсети в качестве критерия соответствия условию правила IP ACL. Значения dstip 0.0.0.0 и dstmask 255.255.255.255 указывают на соответствие любым значениям. Указание **host** A.B.C.D также указывает значение dstip как A.B.C.D и dstmask – как 0.0.0.0.
[precedence precedence | tos tos [tosmask] | dscp dscp]	Указывает TOS для правила IP ACL в зависимости от соответствия приоритета или значений DSCP, используя параметры dscp, precedence, tos/tosmask (tosmask - необязательный параметр).
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	При указании этой опции правило IP ACL фиксирует соответствие флагам TCP. При указании +<tcpflagname> соответствие фиксируется в том случае, если указанный флаг <tcpflagname> установлен в заголовке TCP. При указании -<tcpflagname> соответствие фиксируется в том случае, если указанный флаг <tcpflagname> НЕ установлен в заголовке TCP. При указании «established» соответствие фиксируется в том случае, если указанные биты RST или ACK установлены в заголовке TCP. При указании опции «established» на устройство устанавливаются два правила. Данная опция доступна только с протоколом TCP.
[icmp-type icmp-type [icmp-code icmp-code] | icmp-message icmp-message]	**ПРИМЕЧАНИЕ:** Данная опция доступна только с протоколом ICMP. Указывает критерий соответствия для пакетов ICMP. При указании «icmp-type» правило IP ACL фиксирует соответствие при сообщении ICMP указанного типа (число в диапазоне 0 – 255). При указании «icmp-code» правило IP ACL фиксирует соответствие при сообщении ICMP с указанным кодом (число в диапазоне 0 – 255). Задание «icmp-message» подразумевает, что указаны как icmp-тип, так и icmp-код. Поддерживаются следующие icmp-сообщения: echo, echo-reply, host-redirect, mobile-redirect, net-redirect, net-unreachable, redirect, packet-too-big, portunreachable, source-quench, router-solicitation, routeradvertisement, time-exceeded, ttl-exceeded и unreachable.

Параметр	Описание
[icmp-type icmp-type [icmp-code icmp-code] | icmp-message icmp-message]	ICMP-сообщение декодируется на соответствующий ICMP-тип и ICMP-код в пределах этого типа.
igmp-type igmp-type	**ПРИМЕЧАНИЕ:** Данная опция доступна только с протоколом IGMP. При указании «igmp-type» правило IP ACL фиксирует соответствие сообщения IGMP указанному типу указанного типа (число в диапазоне 0 – 255).
fragments	При указании этой опции правило IP ACL фиксирует соответствие для фрагментированных IP-пакетов.
log	Указывает, что для правила должен вестись журнал.
time-range time-range-name	Позволяет налагать ограничение времени на правило ACL, определяемое параметром time-range-name. Если временной диапазон с указанным именем не существует, и ACL, содержащий это правило, применяется к интерфейсу или привязан к VLAN, тогда правило ACL применяется немедленно. Если временной диапазон с указанным именем существует, и ACL, содержащий это правило, применяется к интерфейсу или привязан к VLAN, тогда правило ACL применяется по наступлению начала указанного диапазона времени. Правило ACL удаляется по истечению временного диапазона с указанным именем.
assign-queue queue-id	Задает параметр assign-queue, идентификатор очереди, которой назначаются пакеты, соответствующие этому правилу.
{mirror | redirect} unit/slot/ port	Задает интерфейс типа «mirror» или «redirect» с указанными unit/slot/port, на который будут, соответственно, копироваться или пересылаться пакеты.
rate-limit rate burst-size	Указывает разрешенную скорость трафика в соответствии с настроенной скоростью в Кбит/с и размером превышения в КБ.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)#ip access-list ip1
(Routing) (Config-ipv4-acl)#permit icmp any any rate-limit 32 16
(Routing) (Config-ipv4-acl)#exit
```

no sequence-number

Данная команда позволяет удалить правило ACL с указанным номером sequence number из ACL.

Формат no sequencenumber

Режим Ipv4-Access-List Config

ip access-group

Данная команда либо присоединяет определенный список IP ACL к интерфейсу или диапазону интерфейсов; либо связывает его с идентификатором VLAN в заданном направлении. Параметр name – имя ACL.

Необязательный параметр «sequence» указывает порядок этого списка IP ACL по отношению к другим IP ACL, уже назначенных этому интерфейсу и направлению. Чем ниже значение, тем выше приоритет. Если указанный параметр «sequence» уже используется для этого интерфейса и направления, указанный IP ACL заменяет текущий IP ACL, используя этот порядковый номер. Если «sequence» для этой команды не указан, используется значение приоритета большее, чем самое большое из уже используемых для этого интерфейса и направления.

Для применения ACL на порте CPU указывается параметр control-plane (необязательно). Пакеты управления IPv4, такие как RADIUS и TACACS+, также отбрасываются из-за неявного правила **deny all**, добавленного в конец списка. Для нейтрализации этого эффекта в конец списка необходимо добавить правила разрешения (permit) для управляющих пакетов IPv4.

ПРИМЕЧАНИЕ: Ключевое слово «control-plane» доступно только в режиме «Global Config».

ПРИМЕЧАНИЕ: Опция out может быть недоступной на некоторых платформах.

По умолчанию нет

Формат ip access-group {accesslistnumber|name} {{control-plane|in|out}|vlan vlan-id {in|out}} [sequence *1-4294967295*]

Режимы Interface Config

Global Config

Параметр	Описание
Accesslistnumbe r	Идентифицирует конкретный список IP ACL. Диапазон - от 1 до 199.
sequence	Значение приоритета этого списка IP ACL по отношению к другим IP ACL, уже назначенных этому интерфейсу и направлению. Диапазон - от 1 до 4294967295.
vlan-id	VLAN ID, связанный с определенным IP ACL в заданном направлении.
name	Имя ACL.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)#ip access-group ip1 control-plane
```

no ip access-group

Данная команда удаляет указанный IP ACL на интерфейсе.

По умолчанию нет

Формат no ip access-group {accesslistnumber|name} {{control-plane|in|out}|vlan vlan-id {in|out}}

Режим Interface Config

Global Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing)(Config)#no ip access-group ip1 control-plane
```

acl-trapflags

Данная команда включает режим ACL trap.

По умолчанию отключено

Формат acl-trapflags

Режим Global Config

no acl-trapflags

Данная команда отключает режим ACL trap.

Формат no acl-trapflags

Режим Global Config

show ip access-lists

Используйте эту команду для просмотра сводной информации обо всех IP ACL, настроенных на коммутаторе. Чтобы просмотреть подробную информацию о конкретном ACL, укажите его номер или имя, используемое для идентификации. Атрибут rate-limit отображает значения гарантированных скорости и размера превышения.

Формат show ip access-lists [accesslistnumber | name]

Режим Privileged EXEC

Термин	Значение
ACL ID/Name	Номер или имя списка ACL.
Rules	Количество настроенных правил для этого ACL.
Direction	Применяется ли ACL к входящему либо исходящему трафику.
Interface(s)	Интерфейсы, к которым применяется ACL.

Термин	Значение
VLAN(s)	VLAN, к которым применяется ACL

При указании номера или имени IP ACL отображается следующая информация:

ПРИМЕЧАНИЕ: Отображаются только настроенные поля ACL. Вывод команды зависит от критериев соответствия, установленных в правилах ACL.

Термин	Значение
Rule Number	Числовой идентификатор для каждого правила, определенного в данном IP ACL.
Action	Действие соответствующее каждому правилу. Возможные значения: Permit (разрешить) и Deny (запретить).
Match All	Применяется ли данный ACL к каждому пакету. Возможные значения: True или False.
Protocol	Протокол для данного правила.
Термин	Значение
ICMP Type	**ПРИМЕЧАНИЕ:** Показывается только для протокола ICMP. Тип сообщения ICMP для этого правила.
Starting Source L4 port	Начальный L4 порт источника.
Ending Source L4 port	Конечный L4 порт источника.
Starting Destination L4 port	Начальный L4 порт назначения.
Ending Destination L4 port	Конечный L4 порт назначения.
ICMP Code	**ПРИМЕЧАНИЕ:** Показывается только для протокола ICMP. Код сообщения ICMP для этого правила.
Fragments	Правило ACL фиксирует соответствие для фрагментированных IP-пакетов.
Committed Rate	Гарантированная скорость, определяемая атрибутом «rate-limit».

Термин	Значение
Committed Burst Size	Гарантированный размер превышения, определяемый атрибутом «rate-limit».
Source IP Address	IP-адрес источника для этого правила.
Source IP Mask	IP-маска источника для этого правила.
Source L4 Port Keyword	Порт источника для этого правила.
Destination IP Address	IP-адрес назначения для этого правила.
Destination IP Mask	IP-маска назначения для этого правила.
Destination L4 Port Keyword	Порт назначения для этого правила.
IP DSCP	Значение, указанное для IP DSCP.
IP Precedence	Значение, указанное для IP Precedence.
IP TOS	Значение, указанное для IP TOS.
Log	Отображается при включении журналирования для данного правила.
Assign Queue	Идентификатор очереди, куда назначаются пакеты, соответствующие критериям данного правила.
Mirror Interface	unit/slot/port, на который копируются пакеты, соответствующие критериям данного правила.
Redirect Interface	unit/slot/port, на который пересылаются пакеты, соответствующие критериям данного правила.
Time Range Name	Имя временного диапазона, если правило IP ACL содержит ссылки на него.
Rule Status	Состояние данного правила IP ACL. Возможные значения: Active (активно) и Inactive (неактивно).

ПРИМЕР: Пример вывода командной строки для данной команды.

```
(Routing) #show ip access-lists ip1
ACL Name: ip1
```

Inbound Interface(s): 1/0/30

Sequence Number: 1

Action permit

Match All.....FALSE

Protocol.....1(icmp)

ICMP Type .....3(Destination Unreachable)

Starting Source L4 port.....80

Ending Source L4 port 85

Starting Destination L4 port 180

Ending Destination L4 port.....185

ICMP Code 0

Fragments.....FALSE

Committed Rate 32

Committed Burst Size.....16

show access-lists

Данная команда отображает информацию о списках IP ACL, IPv6 ACL и MAC ACL для определенного интерфейса и направления. Для указания интерфейса LAG вместо **unit/slot/port** можно использовать lag **lag-intf-num**. Также для указания интерфейса LAG может использоваться lag **lag-intf-num, где lag-intf-num** – это номер порта LAG. Для отображения ACL, назначенных на порт ЦП, используйте ключевое слово **control-plane**.

Формат show access-lists interface {unit/slot/port in|out | control-plane}

Режим Privileged EXEC

Термин	Значение
ACL Type	Тип ACL (IP или MAC).
ACL ID	Имя для MAC ACL либо числовой идентификатор для IP ACL.
Sequence Number	Параметр «sequence» указывает порядок этого списка ACL по отношению к другим ACL, уже назначенных этому интерфейсу и направлению
in|out	in – отображение информации об ACL для определенного интерфейса во входящем направлении. out – отображение информации об ACL для определенного интерфейса в исходящем направлении.

ПРИМЕР: Ниже приведен пример выполнения команды.

(Routing) #show access-lists interface control-plane

```
ACL Type            ACL ID          Sequence Number
-------------------------------------------------------
IPv6                ip61            1
```

show access-lists vlan

Данная команда отображает информацию об ACL для определенного VLAN ID. Параметр **vlan-id** – идентификатор нужной VLAN. Опции {in | out} указывают направление работы VLAN ACL.

Формат show access-lists vlan vlan-id in|out

Режим Privileged EXEC

Термин	Значение
ACL Type	Тип ACL (IP , IPv6 или MAC).
ACL ID	Имя для MAC/IPv6 ACL либо числовой идентификатор для IP ACL.
Sequence Number	Необязательный параметр «sequence» указывает порядок этого списка ACL по отношению к другим ACL, уже назначенных этому интерфейсу и направлению.

10.9. Команды IPv6 Access Control List

В этом разделе описаны команды, используемые для настройки IPv6 Access Control List (ACL). Списки IPv6 ACL отвечают за то, чтобы только авторизованные пользователи имели доступ к определенным ресурсам, и блокируют любые нежелательные попытки достичь сетевых ресурсов.

К спискам IPv6 ACL применяются следующие правила:

- Макимальное количество списков ACL – 100, независимо от их типа.
- Система поддерживает только фреймы типа Ethernet II.
- Максимальное количество правил на один IPv6 ACL зависит от оборудования.

ipv6 access-list

Данная команда создает IPv6 Access Control List (ACL), идентифицируемый по имени (name). Список состоит из полей классификации, определенных для IP-заголовка IPv6-фрейма. Параметр **name** – это строка из букв и цифр длиной от 1 до 31 символа (чувствительно к регистру), которая является уникальным идентификатором ACL. Атрибут rate-limit настраивает гарантированную скорость и гарантированный burst size.

Если IPv6 ACL с таким именем уже существует, команда активирует режим IPv6-Access-List config для обновления существующего ACL.

ПРИМЕЧАНИЕ: После успешного выполнения этой команды режим командной строки меняется на «IPv6 Access-List config».

Формат ipv6 access-list name

Режим Global Config

no ipv6 access-list

Данная команда удаляет из системы IPv6 ACL, определяемый именем (name).

Формат no ipv6 access-list *name*

Режим Global Config

ipv6 access-list rename

Данная команда изменяет имя IPv6 ACL. Параметр **name** – имя существующего IPv6 ACL. Параметр **newname** – это строка из букв и цифр длиной от 1 до 31 символа (чувствительно к регистру), которая является уникальным идентификатором ACL.

Команда не выполняется в том случае, если IPv6 ACL с именем *newname* уже существует.

Формат ipv6 access-list rename *name newname*

Режим Global Config

ipv6 access-list resequence

Данная команда позволяет перенумеровать записи для указанного списка доступа IPv6, с заданным значением инкрементирования, начиная с определенного порядкового номера. Команда используется для редактирования порядковых номеров правил в ACL и изменения порядка внесения записей. Эта команда не сохраняется в конфигурации запуска и не отображается в текущей конфигурации.

По умолчанию 10

Формат ipv6 access-list resequence {name| id } starting-sequence-number increment

Режим Global Config

Параметр	Описание
starting-sequencenumber	Начальный порядковый номер. Диапазон: 1 – 2147483647. Значение по умолчанию - 10.
increment	Инкремент. Диапазон: 1 – 2147483647. Значение по умолчанию - 10.

{deny | permit} (IPv6)

Данная команда создает новое правило для текущего IPv6 ACL. Правило может отклонять или пропускать трафик в соответствии с указанными полями классификации. Как минимум, необходимо указать либо ключевое слово **every** либо адрес протокола, адрес источника и адрес назначения. IPv6-адреса источника и назначения могут быть заменены ключевым словом *any*, чтобы указать совпадение с любым возможным значением в этом поле. Остальные параметры команды являются необязательными, но наиболее часто используемые параметры отображаются в порядке, показанном ниже.

Формат {deny | permit} {every | {{icmpv6 | ipv6 | tcp | udp | 0-255} {*source-ipv6-prefix/ prefix-length* | any | *host source-ipv6-address*} [{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}] {*destination-ipv6-prefix/ prefix-length* | any | *host destination-ipv6-address*} [{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}] [flag [+fin | -fin]

[+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [flow-label value] [icmp-type *icmp-type* [icmp-code *icmp-code*] | icmp-message *icmpmessage*] [routing] [fragments] [sequence *sequence-number*] [dscp *dscp*]}} [log] [assign-queue *queue-id*] [{mirror | redirect} unit/slot/port] [rate-limit *rate burstsize*]

Режим IPv6-Access-List Config

ПРИМЕЧАНИЕ: Неявно выраженное IPv6-правило **deny all IPv6** всегда завершает список ACL.

Дополнительный атрибут команды **permit, rate-limit**, позволяет разрешить только допустимую скорость передачи данных, указанную в Кбит/с, и размер превышения (в КБ).

IPv6 ACL имеют следующие ограничения:

- Диапазоны портов не поддерживаются для исходящих IPv6 ACL.
- Ключевое слово «IPv6 ACL fragment» фиксирует соответствие только в первом заголовке расширения фрагмента IPv6 (next header code 44). Если заголовок фрагмента появляется во втором или последующем заголовке, соответствие не регистрируется.
- Ключевое слово «IPv6 ACL routing» поддерживается только в первом заголовке расширения фрагмента IPv6 (next header code 43). Если заголовок фрагмента появляется во втором или последующем заголовке, соответствие не регистрируется.
- Команда «rate-limit» не поддерживается для исходящих IPv6 ACL.

Параметр	Описание
{deny | permit}	Указывает, запрещает ли данное правило соответствующий трафик или, наоборот, разрешает.
Every	Указывает соответствие любого пакета.
{*protocolkey* | *number*}	Указывает протокол соответствия для правила IPv6 ACL. Текущий список: icmpv6, ipv6, tcp и udp.
source-ipv6-prefix/*prefix-length* | any | *host source-ipv6-address*	Указывает адрес источника IPv6 и длину префикса назначения как условие соответствия правила IPv6 ACL. Значение “::/0 “ указывает на соответствие любым значениям. Указание source-ipv6-address host подразумевает соответствие указанному IPv6-адресу.

Параметр	Описание
source-ipv6-prefix/prefix-length | *any* | *host source-ipv6-address*	Этот аргумент source-ipv6-address должен быть в форме, соответствующей RFC 2373, то есть адрес долежн быть указан в шестнадцатеричном формате, с использованием 16-битных значений между двоеточиями.
[{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}]	**ПРИМЕЧАНИЕ:** Данная опция доступна только с протоколами TCP и UDP. Указывает критерий соответствия L4 порта для условия правила IPv6 ACL. Допускается использование как номера порта (в диапазоне 0 – 65535), так и ключевого слова, которое может быть одним из следующих: Для TCP: bgp, domain, echo, ftp, ftp-data, http, smtp, telnet, www, pop2, pop3 Для UDP:: domain, echo, ntp, rip, snmp, tftp, time, who. Каждое ключевое слово преобразуется системой в соответствующий номер порта. Если задан диапазон, правило IPv6 ACL работает только для L4 портов, попадающих в указанный диапазон. Параметры «startport» и «endport» определяют первый и последний порты диапазона. Они могут иметь значения в диапазоне 0 – 65535. Конечный порт диапазона должен быть не меньше начального. Диапазон портов считается включительно: к нему принадлежат первый и последний порты, а также все порты между ними. При указании «eq» правило IPv6 ACL фиксирует соответствие только для тех случаев, когда номер L4 порта совпадает с указанным портом (порт может быть указан номеров или ключевым словом). При указании «lt» правило IPv6 ACL фиксирует соответствие только для тех случаев, когда номер L4 порта меньше указанного порта. По сути, это эквивалентно диапазону от 0 до <номер указанного порта – 1>. При указании «gt» правило IPv6 ACL фиксирует соответствие только для тех случаев, когда номер L4 порта больше указанного порта. По сути, это эквивалентно диапазону от <номер указанного порта + 1> до 65535. При указании «neq» правило IPv6 ACL фиксирует соответствие только для тех случаев, когда номер L4 порта не совпадает с указанным портом. Добавляются сразу два правила, одно из них – с диапазоном от 0 до <номер указанного порта – 1>, второе – с диапазоном от <номер указанного порта + 1> до 65535..

Параметр	Описание
destination-ipv6-prefix/*prefix-length* | any | *host destination-ipv6-address*	Указывает IPv6-адрес назначения и длину префикса назначения для соответствия условию правила IPv6 ACL. Значение “::/0 “ указывает на соответствие любым значениям. Указание destination-ipv6-address host подразумевает соответствие указанному IPv6-адресу. Этот аргумент destination-ipv6-address должен быть в форме, соответствующей RFC 2373, то есть адрес долежн быть указан в шестнадцатеричном формате, с использованием 16-битных значений между двоеточиями.
sequence *sequence-number*	Указывает порядковый номер для правила ACL. Каждое правило получает свой номер. Данный номер может быть как назначен пользователем, так и сгенерирован устройством. Если для правила не указан порядковый номер, используется номер на 10 больший, чем последний порядковый номер в ACL. Само правило при этом помещается в конец списка. Если это первое правило ACL в данном списке, ему назначается порядковый номер 10. Если сгенерированный порядковый номер превышает максимальное значение, создание правила ACL завершается с ошибкой. Не допускается создание правила, дублирующего уже существующее правило. Правило не может иметь номер sequence number, уже используемый другим правилом. Например, если пользователь добавляет в ACL новое правило без указания порядкового номера, оно помещается в конец списка. Изменяя значение sequence-number, пользователь может изменить позицию этого правила в ACL.
[dscp *dscp*]	Задает значение dscp для соответствия правилу IPv6.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	При указании этой опции правило IPv6 ACL фиксирует соответствие флагам TCP. При указании +<tcpflagname> соответствие фиксируется в том случае, если указанный флаг <tcpflagname> установлен в заголовке TCP. При указании -<tcpflagname> соответствие фиксируется в том случае, если указанный флаг <tcpflagname> НЕ установлен в заголовке TCP. При указании «established» соответствие фиксируется в том случае, если указанные биты RST или ACK установлены в заголовке TCP.

Параметр	Описание
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	При указании опции «established» на устройство устанавливаются два правила. Данная опция доступна только с протоколом TCP.
[icmp-type *icmp-type* [icmp-code *icmp-code]* | icmpmessage *icmp-message*]	**ПРИМЕЧАНИЕ:** Данная опция доступна только с протоколом icmpv6. Указывает критерий соответствия для пакетов ICMP. При указании «icmp-type» правило IPv6 ACL фиксирует соответствие при сообщении ICMP указанного типа (число в диапазоне 0 – 255). При указании «icmp-code» правило IPv6 ACL фиксирует соответствие при сообщении ICMP с указанным кодом (число в диапазоне 0 – 255). Задание «icmp-message» подразумевает, что указаны как icmp-тип, так и icmp-код. Поддерживаются следующие icmp-сообщения: destination-unreachable, echo-reply, echo-request, header, hop-limit, mld-query, mldreduction, mld-report, nd-na, nd-ns, next-header, noadmin, no-route, packet-too-big, port-unreachable, router-solicitation, router-advertisement, routerrenumbering, time-exceeded и unreachable. ICMP-сообщение декодируется в соответствующий ICMP-тип и ICMP-код в пределах этого типа.
Fragments	Указывает соответствие для фрагментированных пакетов IPv6 (пакетов, имеющих в следующем поле заголовка значение 44).
Routing	Указывает соответствие для пакетов IPv6, имеющих расширение маршрутизации в заголовке (имеющих в поле next заголовка значение 43).
Log	Указывает, что для правила должен вестись журнал.

Параметр	Описание
time-range *time-range-name*	Позволяет налагать ограничение времени на правило ACL, определяемое параметром time-range-name. Если временной диапазон с указанным именем не существует, и ACL, содержащий это правило, применяется к интерфейсу или привязан к VLAN, тогда правило ACL применяется немедленно. Если временной диапазон с указанным именем существует, и ACL, содержащий это правило, применяется к интерфейсу или привязан к VLAN, тогда правило ACL применяется по наступлению начала указанного диапазона времени. Правило ACL удаляется по истечению временного диапазона с указанным именем.
assign-queue *queue-id*	Задает параметр assign-queue, идентификатор очереди, которому назначены пакеты, соответствующие этому правилу.
{mirror | redirect} *unit/slot/ port*	Задает интерфейс типа «mirror» или «redirect» с указанными unit/slot/port, на который будут, соответственно, копироваться или пересылаться пакеты.
rate-limit *rate burst-size*	Указывает разрешенную скорость трафика в соответствии с настроенной скоростью в Кбит/с и размером превышения в КБ.

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)#ipv6 access-list ip61
(Routing) (Config-ipv6-acl)#permit udp any any rate-limit 32 16 (Routing) (Config-ipv6-acl)#exit
```

no sequence-number

Данная команда позволяет удалить правило ACL с указанным номером sequence number из ACL.

Формат no sequence-number

Режим Ipv6-Access-List Config

ipv6 traffic-filter

Данная команда либо присоединяет определенный IPv6 ACL, к интерфейсу или диапазону интерфейсов; либо связывает его с идентификатором VLAN в заданном направлении. Параметр *name* – имя существующего IPv6 ACL.

Необязательный параметр «sequence» указывает порядок этого списка IPv6 ACL по отношению к другим IPv6 ACL, уже назначенных этому интерфейсу и направлению. Чем ниже значение, тем выше приоритет. Если указанный параметр «sequence» уже используется для этого интерфейса и направления, указанный IPv6 ACL заменяет текущий IPv6 ACL, используя этот порядковый номер. Если «sequence» для этой команды

не указан, используется значение приоритета большее, чем самое большое из уже используемых для этого интерфейса и направления.

Эта команда, запущенная в режиме «Interface Config», распространяет свое действие на один интерфейс, а в режиме «Global Config» – на все интерфейсы. Ключевое слово vlan действует только в режиме «Global Config». Команда в режиме «Interface Config» доступна только на платформах, поддерживающих независимую конфигурацию очереди CoS для каждого порта.

Для применения ACL на порте CPU указывается параметр control-plane (необязательно). Пакеты управления, такие как IGMPv6, также отбрасываются из-за неявного правила deny all, добавленного в конец списка. Для нейтрализации этого эффекта в конец списка необходимо добавить правила разрешения (permit) для управляющих пакетов IPv6.

ПРИМЕЧАНИЕ: Ключевое слово «control-plane» доступно только в режиме «Global Config».

ПРИМЕЧАНИЕ: Опция *out* может быть недоступной на некоторых платформах.

Формат ipv6 traffic-filter *name* {{control-plane |in|out}|vlan *vlan-id* {in|out}} [sequence *1-4294967295*]

Режимы Global Config

Interface Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)#no ipv6 traffic-filter ip61 control-plane
```

no ipv6 traffic-filter

Данная команда удаляет IPv6 ACL, определяемый именем *name*, из указанного интерфейса и указанного направления.

Формат no ipv6 traffic-filter <*name*{{control-plane | in | out} | vlan <*vlan-id*> {in|out}}

Режимы Global Config

Interface Config

ПРИМЕР: Ниже приведен пример выполнения команды.

```
(Routing) (Config)#no ipv6 traffic-filter ip61 control-plane
```

show ipv6 access-lists

Эта команда отображает список IPv6 ACL и все правила, определенные для него. Параметр [*name*] идентифицирует конкретный IPv6 ACL. Атрибут rate-limit отображает значения гарантированных скорости и размера превышения.

Формат show ipv6 access-lists *[name]*

Режим Privileged EXEC

ПРИМЕЧАНИЕ: Отображаются только настроенные поля ACL. Вывод команды зависит от критериев соответствия, установленных в правилах ACL.

Термин	Значение
Rule Number	Числовой идентификатор правила, определенный в пределах IPv6 ACL.

Термин	Значение
Action	Действите, связанное с каждым правилом. Возможные значения: Permit (разрешить) и Deny (запретить).
Match All	Применяется ли данный ACL к каждому пакету. Возможные значения: True или False.
Protocol	Протокол для данного правила.
Committed Rate	Гарантированная скорость, определяемая атрибутом «rate-limit».
Committed Burst Size	Гарантированный размер превышения, определяемый атрибутом «rate-limit».
Source IP Address	IP-адрес источника для этого правила.
Source L4 Port Keyword	Порт источника для этого правила.
Destination IP Address	IP-адрес назначения для этого правила.
Destination L4 Port Keyword	Порт назначения для этого правила.
IP DSCP	Значение, указанное для IP DSCP.
Термин	Значение
Flow Label	Значение, указанное для метки потока IPv6.
Log	Отображается при включении журналирования для данного правила.
Assign Queue	Идентификатор очереди, куда назначаются пакеты, соответствующие критериям данного правила.
Mirror Interface	*unit/slot/port*, на который копируются пакеты, соответствующие критериям данного правила.
Redirect Interface	*unit/slot/port*, на который пересылаются пакеты, соответствующие критериям данного правила.
Time Range Name	Имя временного диапазона, если правило IPv6 ACL содержит ссылки на него.

Термин	Значение
Rule Status	Состояние данного правила IPv6 ACL. Возможные значения: Active (активно) и Inactive (неактивно).

ПРИМЕР: Вывод командной строки для данной команды.

```
(Routing) #show ipv6 access-lists ip61
ACL Name: ip61
Outbound Interface(s): control-plane
Rule Number: 1
Action .....permit
Match Every.....FALSE
Protocol.....17(udp)
Committed Rate .....32
Committed Burst Size.....16
```

10.10. Команды диапазона времени для Time-Based ACL

Списки ACL, основанные на времени (Time-Based ACL), позволяют настраивать различную работу правил ACL в зависимости от текущего времени. Каждое правило в ACL, за исключением правила неявного запрета, может быть настроено таким образом, чтобы работать только в течение определенного периода времени. Команды временного диапазона позволяют определять конкретные время (часы и дни недели). Диапазон времени идентифицируется по имени, на которое может ссылаться правило ACL.

time-range

Данная команда позволяет создать временной диапазон с указанным именем, состоящий из одного абсолютного и\или одного или нескольких периодических значений времени. Параметр «name» – это строка из букв и цифр длиной от 1 до 31 символа (чувствительно к регистру), которая является уникальным идентификатором диапазона времени. Имя может содержать символы в следующих диапазонах: A-Z, a-z и 0-9, а также специальные символы, такие как пробел, тире и знак подчеркивания.

Если временной диапазон с таким именем уже существует, команда активирует режим «Time-Range config» для обновления существующего диапазона.

ПРИМЕЧАНИЕ: После успешного выполнения данной команды, режим командной строки меняется на Time-Range Config.

Формат time-range *name*

Режим Global Config

no time-range

Данная команда удаляет опеделенный временной диапазон.

Формат no time-range name

Режим Global Config

absolute

Данная команда позволяет добавить во временной диапазон запись об абсолютном значении времени. Один диапазон времени может содержать только одно абсолютное временное значение. Параметры времени основываются на выбранном часовом поясе.

Параметр [**start time date**] указывает дату и время, когда должна вступить в силу конфигурация, ссылающаяся на данный временной диапазон. Время задается в 24-часовом формате, вида «часы:минуты». Например, 8:00 означает восемь часов утра, а 20:00 – восемь часов вечера. Дата определяется в формате «день месяц год». Если начальные время и дата не указаны, конфигурация вступит в силу немедленно.

Параметр [**end time date**] указывает дату и время, когда должна прекратить свое действие конфигурация, ссылающаяся на данный временной диапазон. Время окончания должно наступать позже времени начала. Если конечные время и дата не указаны, конфигурация будет работать бессрочно.

Формат absolute [start *time date*] [end *time date*]

Режим Time-Range Config

no absolute

Данная команда удаляет из диапазона времени запись об абсолютном временном значении.

Формат no absolute

Режим Time-Range Config

periodic

Данная команда позволяет добавить во временной диапазон запись о периодическом значении времени. Параметры времени основываются на выбранном часовом поясе.

Первое упоминание аргумента **days-of-the-week** – это день (или дни), в которые будет запускаться конфигурация, ссылающаяся на данный временной диапазон. Второе появление этого аргумента задает конечный день, когда конфигурация будет прекращать свое действие. Если конечное значение «days-of-the-week» совпадает с начальным, его можно не указывать.

Этот аргумент может представлять собой один день либо комбинацию дней: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday. Другие возможные значения:

- daily — с понедельника (Monday) по воскресенье (Sunday)
- weekdays — с понедельника (Monday) по пятницу (Friday)
- weekend — суббота (Saturday) и воскресенье (Sunday)

Первое упоминание аргумента **time** – это временное значение в формате «часы:минуты», в которые будет запускаться конфигурация, ссылающаяся на данный временной диапазон. Второе появление этого аргумента – конечное временное значение в формате «часы:минуты», когда конфигурация будет прекращать свое действие.

Время выражается в 24-часовом формате. Например, 8:00 означает восемь часов утра, а 20:00 – восемь часов вечера.

Формат periodic *days-of-the-week time* to *time*

Режим Time-Range Config

no periodic

Данная команда позволяет удалить из временного диапазона запись о периодическом значении времени

Формат no periodic *days-of-the-week time* to *time*

Режим Time-Range Config

show time-range

Данная команда отображает временной диапазон со всеми определенными абсолютными и периодическими записями. Параметр *name* идентифицирует конкретный диапазон времени. Если параметр *name* не задан, то показываются все диапазоны времени, определенные в системе.

Формат show time-range [name]

Режим Privileged EXEC

Следующая информация будет отображена, если не указан конкретный временной диапазон.

Термин	Значение
Admin Mode	Административный режим функции диапазона времени: включена или выключена
Current number of all Time Ranges	Количество временных диапазонов, настроенных в системе.
Maximum number of all Time Ranges	Максимальное количество временных диапазонов, которые могут быть настроены в системе.
Time Range Name	Имя диапазона времени.
Status	Состояние диапазона времени. Может быть: active (активное) или inactive (неактивное).
Periodic Entry count	Количество периодических записей, настроенных для диапазона времени.
Absolute Entry	Указывает, настроены ли для данного диапазона какие-либо абсолютные значения.

10.11. Команды Auto-Voice over IP

В этом разделе описаны команды, которые используются для настройки Auto-Voice over IP (VoIP). Функция AutoVoIP явно отбирает потоки VoIP в коммутаторах Ethernet и предоставляет им лучший класс обслуживания, чем обычному трафику. Когда на интерфейсе включается функция Auto-VoIP, интерфейс сканирует входящий трафик на следующие протоколы управления вызовами:

- Session Initiation Protocol (SIP)
- H.323
- Skinny Client Control Protocol (SCCP)

При обнаружении протокола управления вызовами коммутатор назначает трафик этого сеанса самой приоритетной очереди CoS, которая обычно используется для чувствительного к времени трафика.

auto-voip

Данная команда используется для настройки режима auto VoIP. Поддерживаемые режимы: protocol-based и oui-based. Protocol-based auto VoIP приоритизирует голосовые данные на основе L4 порта, используемого для голосового сеанса. OUI based auto VoIP приоритизирует трафик телефона на основе известного OUI данного телефона.

Оба режима могут быть включены одновременно. В таком случае, если подключенный OUI телефона является одним из настроенных OUI, то голосовые данные приоритизируются с использованием OUI Auto VoIP, в противном случае для определения приоритетности голосовых данных используется Protocol-based auto VoIP.

Если на порту отключается protocol-based auto VoIP, то активные сеансы очищаются.

По умолчаню oui-based

Формат auto-voip [protocol-based | oui-based]

Режим Global Config

Interface Config

no auto-voip

Используйте **no**-форму команды, чтобы вернуть значения по умолчанию.

auto-voip oui

Данная команда используется для настройки OUI для Auto VoIP. Трафик из настроенного OUI получает высший приоритет перед прочим трафиком. Параметр **oui-prefix** - уникальный OUI, который идентифицирует производителя или поставщика устройства. OUI указывается в виде трех октетов, представляющих собой двузначные шестнадцатеричные числа, разделенные двоеточиями. Параметр **string** – описание OUI, идентифицирующее производителя или поставщика, связанного с OUI.

По умолчанию Присутствует список известных OUI.

Формат auto-voip oui oui-prefix oui-desc string

Режим Global Config

ПРИМЕР: Следующий пример иллюстрирует добавление OUI в таблицу.

```
(Routing) (Config)#auto-voip oui 00:03:6B desc "Cisco VoIPPhone"
```

no auto-voip oui

Используйте **no**-форму команды, чтобы удалить настроенный префикс OUI из таблицы.

Формат no auto-voip oui *oui-prefix*

Режим Global Config

auto-voip oui-based priority

Данная команда используется для глобальной настройки приоритета OUI based auto VoIP. Если OUI телефона соответствует одному из настроенных OUI, приоритет трафика с телефона изменяется на приоритет OUI, сконфигурированный с помощью этой команды. Параметр **priority-value** – значение приоритета 802.1p, используемое для трафика, соответствующее значению в списке OUI. Если интерфейс обнаруживает соответствие OUI, коммутатор назначает трафик в этом сеансе классу трафика, соответствующему этому значению приоритета. Классы трафика с более высоким значением обычно используются для чувствительного к времени трафика.

По умолчанию Самое высокое из возможных значений приоритета.

Формат auto-voip oui-based priority priority-value

Режим Global Config

no auto-voip oui-based priority

Используйте **no-**форму команды, чтобы удалить глобально настроенный приоритет OUI based auto VoIP.

Формат no auto-voip oui *oui-prefix*

Режим Global Config

auto-voip protocol-based

Данная команда используется для настройки глобального перемаркирования приоритета класса трафика protocol-based auto VoIP. При настроенном перемаркировании приоритета, голосовые данные сеанса перемаркируются значением приоритета, настроенным данной командой. Параметр **remark-priority** – значение приоритета 802.1p, используемое для трафика protocol-based VoIP. Если интерфейс обнаруживает протокол управления вызовами, устройство отмечает трафик в этом сеансе указанным значением приоритета 802.1p, чтобы гарантировать, что голосовой трафик всегда получает наивысший приоритет на протяжении всего пути.

Значение *tc* – класс трафика, используемый для protocol-based VoIP. Если интерфейс обнаруживает протокол управления вызовами, устройство назначает трафик в этом сеансе настроенной очереди Class of Service (CoS). Классы трафика с более высоким значением обычно используются для чувствительного к времени трафика. Очередь CoS, связанная с указанным классом трафика, должна быть настроена с соответствующим распределением полосы пропускания, чтобы обеспечить приоритетную обработку VoIP-трафика.

ПРИМЕЧАНИЕ: Для перемаркирования исходящего голосового трафика необходимо настроить тегирование на портах с включенным auto VoIP.

По умолчанию Traffic class 7

Формат auto-voip protocol-based {remark remark-priority | traffic-class tc}

Режим Global Config

Interface Config

no auto-voip protocol-based

Данная команда используется для сброса настроек глобального перемаркирования приоритета класса трафика protocol-based auto VoIP на значения по умолчанию.

Формат no auto-voip protocol-based {remark remark-priority | traffic-class tc}

Режим Global Config

Interface Config

auto-voip vlan

Данная команда используется для настройки глобального идентификатора Auto VoIP VLAN ID. Поведение VLAN зависит от настроенного режима Auto VoIP. Auto VoIP VLAN – это VLAN, используемая для отделения трафика VoIP от прочего не голосового трафика. Трафик VoIP, соответствующий известному OUI, назначается данной VoIP VLAN.

По умолчанию Нет

Формат auto-voip vlan vlan-id

Режим Global Config

no auto-voip vlan

Используйте **no**-форму команды для сброса auto-VoIP VLAN ID на значение по умолчанию.

Формат no auto-voip vlan

Режим Global Config

show auto-voip

Данная команда отображает настройки auto VoIP на одном или нескольких интерфейсах коммутатора.

Формат show auto-voip {protocol-based|oui-based} interface {unit/slot/port|all}

Режим Privileged EXEC

Поле	Описание
VoIP VLAN ID	Глобальный идентификатор VoIP VLAN.
Prioritization Type	Тип приоритизациии, используемый для голосового трафика.
Class Value	• Если тип Prioritization Type настроен как traffic-class, то данное значение – это значение очереди. • Если тип Prioritization Type настроен как remark, то данное значение - это приоритет 802.1p, используемый для перемаркирования голосового трафика.
Priority	Приоритет 802.1p. Поле действительно для OUI auto VoIP.
AutoVoIP Mode	Режим Auto VoIP на интерфейсе.

ПРИМЕР: Пример вывода командной строки для данной команды.

```
(Routing)# show auto-voip protocol-based interface all
```

VoIP VLAN Id 2
Prioritization Type .....traffic-class
Class Value 7

Interface	Auto VoIP Mode	Operational Status
0/1	Disabled	Down
0/2	Disabled	Down
0/3	Disabled	Down
0/4	Disabled	Down

ПРИМЕР: Пример вывода командной строки для данной команды.

(Routing)# show auto-voip oui-based interface all
VoIP VLAN Id 2
Priority.....7

Interface	Auto VoIP Mode	Operational Status
0/1	Disabled	Down
0/2	Disabled	Down
0/3	Disabled	Down
0/4	Disabled	Down
0/5	Disabled	Down

Компонент	Сообщение	Причина
BSP	Event(0xaaaaaaaa)	Коммутатор перезагрузился.
BSP	Starting code...	Инициализация BSP завершена, запускается приложение коммутатора.

Таблица NIM Log Mes

Компонент	Сообщение	Причина
NIM	NIM: L7_ATTACH out of order for interface unit x slot x port x	Создание интерфейса не соответствует правилам.
NIM	NIM: Failed to find interface at unit x slot x port x for event(x)	Отсутствует сопоставление между USP и номером интерфейса.

Компонент	Сообщение	Причина
NIM	NIM: L7_DETACH out of order for interface unit x slot x port x	Создание интерфейса не соответствует правилам.
NIM	NIM: L7_DELETE out of order for interface unit x slot x port x	Создание интерфейса не соответствует правилам.

show auto-voip oui-table

Данная команда отображает информацию о таблице VoIP oui.

Формат show auto-voip oui-table

Режим Privileged EXEC

Параметр	Описание
OUI	OUI MAC-адреса источника.
Status	Запись по умолчанию или пользовательская.
OUI Description	Описание OUI.

ПРИМЕР: Пример вывода командной строки для данной команды.

```
(Routing)# show auto-voip oui-table
OUI                 Status              Description
------------------------------------------------------------------------
00:01:E3            Default             SIEMENS
00:03:6B            Default             CISCO1
00:01:01            Configured          VoIP phone
```

11. СООБЩЕНИЯ ЖУРНАЛА КОММУТАТОРА

В этой главе перечислены сообщения журнала коммутатора, а также информация о причине каждого сообщения. Каждое отдельное сообщение журнала не предполагает каких-либо однозначных ответных действий. Если диагностируется проблема, набор сообщений в журнале событий (также как и понимание конфигурации системы) помогает определить основную причину проблемы. Сообщения журнала приводятся в обратном порядке (сначала самые последние).

ПРИМЕЧАНИЕ: Данный раздел не является полным описанием всех возможных сообщений журнала.

Раздел состоит из следующих глав:

- Ядро
- Утилиты
- Управление
- Комутация
- QoS
- Стекирование
- Технологии
- Поддержка ОС

11.1. Ядро

Сообщения журнала BSP

Компонент	Сообщение	Причина
BSP	Event(0xaaaaaaaa)	Коммутатор перезагрузился.
BSP	Starting code	Инициализация BSP завершена, запускается приложение коммутатора.

Сообщения журнала NIM

Компонент	Сообщение	Причина
NIM	NIM: L7_ATTACH out of order for interface unit x slot x port x	Создание интерфейса не произошло
NIM	NIM: Failed to find interface at unit x slot x port x for event(x)	Отсутствует сопоставление между USP и номером интерфейса.

Компонент	Сообщение	Причина
NIM	NIM: L7_DETACH out of order for interface unit x slot x port x	Создание интерфейса не произошло
NIM	NIM: L7_DELETE out of order for interface unit x slot x port x	Создание интерфейса не произошло
NIM	NIM: event(x),intf(x),component(x), in wrong phase	Событие было выдано NIM во время неверной фазы конфигурации (возможно, фазы 1, 2 или WMU).
NIM	NIM: Failed to notify users of interface change	Событие не было передано в систему.
NIM	NIM: failed to send message to NIM message Queue.	Очередь сообщений NIM заполнена либо не существует.
NIM	NIM: Failed to notify the components of L7_CREATE event	Интерфейс не создан.
NIM	NIM: Attempted event (x), on USP x.x.x before phase 3	Компонент выдал событие интерфейса во время неверной фазы инициализации.
NIM	NIM: incorrect phase for operation	Вызов API был сделан во время неправильной фазы инициализации.
NIM	NIM: Component(x) failed on event(x) for interface	Компонент ответил на событие интерфейса индикацией отказа.

Компонент	Сообщение	Причина
NIM	NIM: Timeout event(x), interface remainingMask = xxxx	Компонент не ответил до наступления таймаута NIM.

Сообщения журнала SIM

Компонент	Сообщение	Причина
SIM	IP address conflict on service port/network address x.x.x.x. Conflicting host MAC address is xx:xx:xx:xx:xx:xx	Это сообщение появляется когда обнаружен конфликт адреса на LAN для сервисного или сетевого порта.

Сообщения системного журнала

Компонент	Сообщение	Причина
SYSTEM	Configuration file switch.cfg size is 0 (zero) bytes	Конфигурационный файл не может быть прочитан. Это сообщение может возникать в системе, в которой ни разу не сохранено конфигураций, либо они все были удалены.
SYSTEM	could not separate SYSAPI_CONFIG_FILENAME	Конфигурационный файл не может быть прочитан. Это сообщение может возникать в системе, в которой ни разу не сохранено конфигураций, либо они все были удалены.
SYSTEM	Building defaults for *file file name version version num*	Конфигурации не существует, либо она не может быть прочитана. Будет использована конфигурация по умолчанию. Имя файла и версия указаны.
SYSTEM	File filename: same version (version num) but the sizes (version size – expected version size) differ	Загруженный конфигурационный файл имеет не тот размер, который ожидается, учитывая номер версии. Это сообщение указывает на то, что для конфигурационного файла нужно провести процедуру миграции на подходящую версию. Это сообщение также может появляться после обновлениия на более новую версию.

Компонент	Сообщение	Причина
SYSTEM	Migrating config file filename from version version num to version num	Для конфигурационного файла была произведена процедура миграции с одной из предшествующих версий. Указываются номера прошлой и текущей версий. Это сообщение также может появляться после обновлениия на более новую версию.
SYSTEM	Building Defaults	Конфигурации не существует, либо она не может быть прочитана. Будет использована конфигурация по умолчанию.
SYSTEM	sysapiCfgFileGet failed size = expected size file version = expected version	Конфигурации не существует, либо она не может быть прочитана. За этим сообщением, как правило, следует сообщение о том, что будет использована конфигурация по умолчанию

11.2. Утилиты

Сообщения Trap Mgr Log

Компонент	Сообщение	Причина
Trap Mgr	Link Up/Down: unit/slot/port	Состояние линка интерфейса изменилось.

Сообщения журнала DHCP фильтрации

Компонент	Сообщение	Причина
DHCP Filtering	Unable to create r/w lock for DHCP	Невозможно создать семафор, используемый для структуры конфигурации фильтрации DHCP.
DHCP Filtering	Unable to create r/w lock for DHCP	Невозможно создать семафор, используемый для структуры конфигурации фильтрации DHCP.
DHCP Filtering	Failed to register with nv Store.	Не удалось зарегистрировать функции сохранения и восстановления для сохранения конфигурации.
DHCP Filtering	Failed to register with NIM	Не удалось зарегистрироваться в NIM для функций обратного вызова интерфейса.

Компонент	Сообщение	Причина
DHCP Filtering	Error on call to sysapiCfgFile Write file	Ошибка при попытке сохранить конфигурацию.

Сообщения журнала NVStore

Компонент	Сообщение	Причина
NVStore	Building defaults for file XXX	Конфигурационный файл компонента не существует или контрольная сумма файла некорректна, поэтому построен файл конфигурации по умолчанию компонента.
NVStore	Error on call to osapiFsWrite routine on file XXX	Либо файл не может быть открыт, либо контроллер ввода\ввода операционной системы возвратил ошибку при попытке записать в файл
NVStore	File XXX corrupted from file system Checksum mismatch.	Вычисленная контрольная сумма конфигурационного файла компонента в файловой системе не соответствует контрольной сумме файла в памяти.
NVStore	Migrating config file XXX from version Y to Z	Было обнаружено несоответствие версии файла конфигурации, запущена процедура миграции версии.

Сообщения журнала RADIUS

Компонент	Сообщение	Причина
RADIUS	RADIUS: Invalid data length - xxx	Клиент RADIUS получил недопустимое сообщение от сервера.
RADIUS	RADIUS: Failed to send the request	Проблема при попытке установки связи с сервером RADIUS.
RADIUS	RADIUS: Failed to send all of the request	Проблема связи с сервером RADIUS при передаче.
RADIUS	RADIUS: Could not get the Task Sync semaphore!	Проблема с ресурсами службы RADIUS.

Компонент	Сообщение	Причина
RADIUS	RADIUS: Buffer is too small for response processing	Клиент RADIUS попытался сформировать ответ больший, чем позволяют ресурсы.
RADIUS	RADIUS: Could not allocate accounting requestInfo	Проблема с ресурсами службы RADIUS.
RADIUS	RADIUS: Could not allocate requestInfo	Проблема с ресурсами службы RADIUS.
RADIUS	RADIUS: osapiSocketRecvFrom returned error	Ошибка при попытке чтения данных с сервера RADIUS.
RADIUS	RADIUS: Accounting-Response failed to validate, id = xxx	Клиент RADIUS получил недопустимое сообщение от сервера.
RADIUS	RADIUS: User (xxx) needs to respond for challenge	Получен неожиданный вызов для настроенного пользователя.
RADIUS	RADIUS: Could not allocate a buffer for the packet	Проблема с ресурсами службы RADIUS.
RADIUS	RADIUS: Access-Challenge failed to validate, id = xxx	Клиент RADIUS получил недопустимое сообщение от сервера.
RADIUS	RADIUS: Failed to validate MessageAuthenticator, id = xxx	Клиент RADIUS получил недопустимое сообщение от сервера.
RADIUS	RADIUS: Access-Accept failed to validate, id = xxx	Клиент RADIUS получил недопустимое сообщение от сервера.
RADIUS	RADIUS: Invalid packet length – xxx	Клиент RADIUS получил недопустимое сообщение от сервера.
RADIUS	RADIUS: Response is missing Message-Authenticator, id = xxx	Клиент RADIUS получил недопустимое сообщение от сервера.
RADIUS	RADIUS: Server address doesn't match configured server	Клиент RADIUS получил ответ от ненастроенного сервера.

Журнал TACACS+. Сообщения

Компонент	Сообщение	Причина
TACACS+	TACACS+: authentication error, no server to contact	Требуется запрос TACACS+, но нет настроенных серверов.
TACACS+	TACACS+: connection failed to server x.x.x.x	Запрос TACACS+ отправлен на сервер x.x.x.x, но ответ не получен.
TACACS+	TACACS+: no key configured to encrypt packet for server x.x.x.x	Для указанного сервера не настроен ключ.
TACACS+	TACACS+: received invalid packet type from server	Получен пакет неподдерживаемого типа.
TACACS+	TACACS+: invalid major version in received packet.	Существенное несоответствие версий.
TACACS+	TACACS+: invalid minor version in received packet.	Несущественное несоответствие версий.

Сообщения журнала LLDP

Компонент	Сообщение	Причина
LLDP	lldpTask(): invalid message type:xx. xxxxxx:xx	Получен неподдерживаемый пакет LLDP.

Сообщения журнала SNTP

Компонент	Сообщение	Причина
SNTP	SNTP: system clock synchronized on %s UTC	Указывает, что SNTP успешно синхронизировал время с сервером.

Сообщения журнала клиента DHCPv6

Компонент	Сообщение	Причина
DHCP6 Client	ip6Map dhcp add failed.	Это сообщение появляется, когда обновление арендованного IP-адреса DHCP в IP6Map завершается с ошибкой.

Сообщения журнала клиента DHCPv6

Компонент	Сообщение	Причина
DHCP6 Client	osapiNetAddrV6Add failed on interface xxx.	Это сообщение появляется, когда обновление арендованного IP-адреса DHCP в ядре IP стека завершается с ошибкой.
DHCP6 Client	Failed to add DNS Server xxx to DNS Client.	Это сообщение появляется при ошибке обновления адреса сервера DNS6, выданного DHCPv6-сервером DNS6-клиенту.
DHCP6 Client	Failed to add Domain name xxx to DNS Client.	Данное сообщение появляется при ошибке обновления доменного имени DNS6, выданного DHCPv6-сервером DNS6-клиенту.

Сообщения журнала клиента DHCPv4

Компонент	Сообщение	Причина
DHCP4 Client	Unsupported subOption (xxx) in Vendor Specific Option in received DHCP pkt	Это сообщение появляется при получении сообщения DHCP-сервера, содержащего неподдерживаемую опцию Vendor Option.
DHCP4 Client	Failed to acquire an IP address on xxx; DHCP Server did not respond.	Это сообщение появляется, когда попытка аренды IP-адреса DHCP-клиентом завершается неудачей.
DHCP4 Client	DNS name server entry add failed.	Это сообщение появляется при ошибке обновления имени сервера DNS, выданного DHCP-сервером DNS-клиенту.
DHCP4 Client	DNS domain name list entry addition failed.	Это сообщение появляется при ошибке обновления списка доменных имен DNS, выданного DHCP-сервером DNS-клиенту.

Компонент	Сообщение	Причина
DHCP4 Client	Interface xxx Link State is Down. Connect the port and try again.	Это сообщение появляется, когда на сетевом протоколе настроен DHCP без каких-либо активных линков в управляющей VLAN.

11.3. Управление

Сообщения журнала SNMP

Компонент	Сообщение	Причина
SNMP	EDB Callback: Unit Join: x.	К стеку присоединилось новое устройство.

Сообщения журнала EmWeb

Компонент	Сообщение	Причина
EmWeb	EMWEB (Telnet): Max number of Telnet login sessions exceeded	Пользователь попытался подключиться через telnet, когда максимальное количество сеансов telnet уже было достигнуто.
EmWeb	EMWEB (SSH): Max number of SSH login sessions exceeded	Пользователь попытался подключиться через SSH, когда максимальное количество сеансов SSH уже было достигнуто.
EmWeb	Handle table overflow	Используются все доступные соединения EmWeb, соединение не может быть установлено.
EmWeb	ConnectionType EmWeb socket accept() failed: errno	Отказ принятия сокета для указанного типа подключения.
EmWeb	ewsNetHTTPReceive failure in NetReceiveLoop() - closing connection.	Ошибка сокета при приёме.
EmWeb	EmWeb: connection allocation failed	Ошибка распределения памяти для нового подключения.

Компонент	Сообщение	Причина
EmWeb	EMWEBTransmitPending: error sending data ewa EWOULDBLOCK NetHTTPEnd: internal error – handle in Handle table	Ошибка сокета при отправке. Недействительный индекс обращения к EmWeb.
EmWeb	ewsNetHTTPReceive:recvBufCnt exceeds MAX_QUEUED_RECV_BUFS!	Буфер приёма достиг своего лимита. Некорректный запрос либо DoS-атака.
EmWeb	EmWeb accept: XXXX	Ошибка функции приема нового SSH-соединения. XXXX – информация об ошибке.

Сообщения журнала CLI_UTIL

Компонент	Сообщение	Причина
CLI_UTIL	Telnet Send Failed errno = 0x%x	Ошибка при попытке отправки текстовой строки Telnet-клиенту.
CLI_UTIL	osapiFsDir failed	Ошибка при попытке получить информацию о директории из директории раздела.

Сообщения журнала WEB

Компонент	Сообщение	Причина
WEB	Max clients exceeded	Данное сообщение отображается при достижении максимального количества клиентских подключений java к коммутатору.
WEB	Error on send to sockfd XXXX, closing connection	Не удалось отправить данные клиентам java через сокет.
WEB	# (XXXX) Form Submission Failed. No Action Taken.	Представление формы не удалась, никаких действий не предпринято. XXXX указывает файл.

Компонент	Сообщение	Причина
WEB	ewaFormServe_file_download() - WEB Unknown return code from tftp download result	В ходе загрузки файла через Веб-интерфейс с использованием TFTP произошла неизвестная ошибка.
WEB	ewaFormServe_file_upload() - Unknown return code from tftp upload result	В ходе выгрузки файла через Веб-интерфейс с использованием TFTP произошла неизвестная ошибка.
WEB	Web UI Screen with unspecified access attempted to be brought up	Не удалось получить авторизацию для приложения, предоставленную EmWeb /Серверу приложением в ewsAuthRegister (). Указанная Веб-страница будет обслуживаться в режиме только для чтения.

Сообщения журнала CLI_WEB_MGR

Компонент	Сообщение	Причина
CLI_WEB_MGR	File size is greater than 2K	Размер файла баннера превышает 2 КБ.
CLI_WEB_MGR	No. of rows greater than allowed maximum of XXXX	Количество строк превышает допустимый максимум строк.

Сообщения журнала SSHD

Компонент	Сообщение	Причина
SSHD	SSHD: Unable to create the global (data) semaphore	Не удалось создать семафор для глобальной защиты данных.
SSHD	SSHD: Msg Queue is full, event = XXXX	Не удалось отправить сообщение в очередь SSHD, поскольку очередь сообщений заполнена. XXXX указывает событие, которое нужно отправить.

Компонент	Сообщение	Причина
SSHD	SSHD: Unknown UI event in message, event = XXXX	Не удалось отправить событие пользовательского интерфейса в соответствующую функцию SSHD, так как это недопустимое событие. XXXX указывает событие, которое нужно отправить.

Сообщения журнала SSLT

Компонент	Сообщение	Причина
SSLT	SSLT: Exceeded maximum, ssltConnectionTask	Превышен максимум допустимых SSLT-соединений.
SSLT	SSLT: Error creating Secure server socket6	Не удалось создать безопасный сокет сервера для IPV6.
SSLT	SSLT: Can't connect to unsecure server at XXXX, result = YYYY, errno = ZZZZ	Не удалось открыть соединение с незащищенным сервером. XXXX - это небезопасный адрес сокета сервера. YYYY - результат, возвращаемый функцией соединения, а ZZZZ - код ошибки.
SSLT	SSLT: Msg Queue is full, event = XXXX	Не удалось отправить сообщение в очередь SSLT, поскольку очередь сообщений заполнена. XXXX указывает событие, которое нужно отправить.
SSLT	SSLT: Unknown UI event in message, event = XXXX	Не удалось отправить полученное событие пользовательского интерфейса в соответствующую функцию SSLT, так как это недопустимое событие. XXXX указывает событие, которое нужно отправить.
SSLT	ssltApiCnfgrCommand: Failed calling ssltIssueCmd.	Не удалось отправить сообщение в очередь SSLT.

Компонент	Сообщение	Причина
SSLT	SSLT: Error loading certificate from file XXXX	Ошибка при загрузке SSL-сертификата из указанного файла. XXXX указывает файл, из которого считывается сертификат.
SSLT	SSLT: Error loading private key from file	Ошибка при загрузке приватного ключа для SSL-соединения.
SSLT	SSLT: Error setting cipher list (no valid ciphers)	Ошибка при загрузке набора шифров.
SSLT	SSLT: Could not delete the SSL semaphores	Не удалось удалить семафоры SSL во время очистки всех ресурсов, связанных с семафорами OpenSSL Locking.

Сообщения журнала User_Manager

Компонент	Сообщение	Причина
User_Manager	User Login Failed for XXXX	Процедура аутентификации не удалась. XXXX указывает имя пользователя.
User_Manager	Access level for user XXXX could not be determined. Setting to Level 1.	Недопустимый уровень доступа, указанный для пользователя. Уровень доступа установлен на Уровень 1. XXXX указывает имя пользователя.
User_Manager	Could not migrate config file XXXX from version YYYY to ZZZZ. Using defaults.	Не удалось произвести процедуру миграции для файла конфигурации. XXXX - это имя файла конфигурации. YYYY - номер старой версии, ZZZZ - номер новой.

11.4. Комутация

Сообщений журнала резервируемых портов

Компонент	Сообщение	Причина
Protected Ports	Protected Port: failed to save configuration	Конфигурация защищенного порта не может быть сохранена.
Protected Ports	protectedPortCnfgrInitPhase1Process: Unable to create r/w lock for protected Port	Ошибка protectedPortCfgRWLock.
Protected Ports	protectedPortCnfgrInitPhase2Process: Unable to register for VLAN change callback	Ошибка nimRegisterIntfChange с VLAN
Protected Ports	Cannot add interface xxx to group yyy	Интерфейс не может быть добавлен в указанную группу.
Protected Ports	unable to set protected port group	Ошибка при попытке добавления маски интерфейса на уровне драйвера.
Protected Ports	Cannot delete interface xxx from group yyy	Ошибка при попытке удаления интерфейса из группы.
Protected Ports	Cannot update group YYY after deleting interface XXX	Ошибка обновления группы при удалении интерфейса.
Protected Ports	Received an interface change callback while not ready to receive it	Вызов смены интерфейса пришел до того, как компонент защищенного порта будет готов.

Сообщения журнала IP Subnet VLANS

Компонент	Сообщение	Причина
IP subnet VLANs	ERROR vlanIpSubnetSubnetValid:Invalid subnet	Это происходит, когда неверное сочетание подсети и маски подсети поступает из командной строки.

Компонент	Сообщение	Причина
IP subnet VLANs	IP Subnet Vlans: failed to save configuration	Это сообщение появляется, если не удалось выполнить сохранение параметров VLAN подсети.
IP subnet VLANs	vlanIpSubnetCnfgrInitPhase1Process: Unable to create r/w lock for vlanIpSubnet	Это сообщение появляется при ошибке блокировки чтения/записи.
IP subnet VLANs	vlanIpSubnetCnfgrInitPhase2Process: Unable to register for VLAN change callback	Это сообщение появляется когда компонент не может зарегистировать уведомление об изменении vlan.
IP subnet VLANs	vlanIpSubnetCnfgrFiniPhase1Process: could not delete avl semaphore	Попытка семафора удалить данный компонент не удалась.
IP subnet VLANs	vlanIpSubnetDtlVlanCreate: Failed	Попытка добавить запись в таблицу не удалась.
IP subnet VLANs	vlanIpSubnetSubnetDeleteApply: Failed	Попытка добавить запись в таблицу не удалась.
P subnet VLANs	vlanIpSubnetVlanChangeCallback: Failed to add an Entry	Попытка добавить запись для vlan не удалась.
P subnet VLANs	vlanIpSubnetVlanChangeCallback: Failed to delete an Entry	Попытка удалить запись для события уведомления о удалении vlan.

Сообщений журнала Mac-based VLAN

Компонент	Сообщение	Причина
MAC based VLANs	MAC VLANs: Failed to save configuration	Не удалось сохранить конфигурацию Mac vlan.
MAC based VLANs	vlanMacCnfgrInitPhase1Process: Unable to create r/w lock for vlanMac	Это сообщение появлется, при ошибке создания блокировки чтения/записи для vlanMac
MAC based VLANs	Unable to register for VLAN change callback	Этот компонент не может зарегистрироваться для уведомлений об изменении vlan.

Компонент	Сообщение	Причина
MAC based VLANs	vlanMacCnfgrFiniPhase1Process: could not delete avl semaphore	Ошибка удаления семафора этого компонента.
MAC based VLANs	vlanMacAddApply: Failed to add an entry	Попытка добавить запись в таблицу не удалась.
MAC based VLANs	vlanMacDeleteApply: Unable to delete an Entry	Попытка удалить запись из таблицы не удалась.
MAC based VLANs	vlanMacVlanChangeCallback: Failed to add an entry	Попытка добавить запись для уведомления о добавлении vlan не удалась.
MAC based VLANs	vlanMacVlanChangeCallback: Failed to delete an entry	Попытка добавить запись для уведомления об удалении vlan не удалась.

Сообщения журнала 802.1X

Компонент	Сообщение	Причина
802.1X	function: Failed calling dot1xIssueCmd	Очередь сообщений 802.1X заполенена.
802.1X	function: EAP message not received from server	Север RADIUS не отправил требуемого сообщения EAP.
802.1X	function: Out of System buffers	802.1X не может обработать/передать сообщение из-за нехватки внутренних буферов.
802.1X	function: could not set state to authorized/ unauthorized, intf xxx	Не удалось установить статус авторизации порта.
802.1X	dot1xApplyConfigData: Unable to enable/ disable dot1x in driver	Не удалось включить/отключить 802.1X.
802.1X	dot1xSendRespToServer: dot1xRadiusAccessRequestSend failed	Не удалось отправить сообщение на RADIUS-сервер.
802.1X	dot1xRadiusAcceptProcess: error calling radiusAccountingStart, ifIndex = xxx	Не удалось отправить accounting start на RADIUS-сервер.

Компонент	Сообщение	Причина
802.1X	function: failed sending terminate cause, intf xxx	Не удалось отправить accounting stop на RADIUS-сервер.

Сообщения журнала IGMP Snooping

Компонент	Сообщение	Причина
IGMP Snooping	function: osapiMessageSend failed	Очередь сообщений IGMP Snooping заполнена.
IGMP Snooping	Failed to set global igmp snooping mode to xxx	Не удалось установить глобальный режим отслеживания IGMP из-за того, что очередь сообщений заполнена.
IGMP Snooping	Failed to set igmp snooping mode xxx for interface yyy	Не удалось настроить IGMP Snooping на интерфейсе по причине переполнения очереди сообщений.
IGMP Snooping	Failed to set igmp mrouter mode xxx for interface yyy	Не удалось установить режим присутствия многоадресного маршрутизатора на интерфейсе из-за того, что очередь сообщений IGMP Snooping заполнена.
IGMP Snooping	Failed to set igmp snooping mode xxx for vlan yyy	Не удалось установить режим VLAN IGMP Snooping из-за того, что очередь сообщений заполнена.
IGMP Snooping	Failed to set igmp mrouter mode%d for interface xxx on Vlan yyy	Не удалось установить режим присутствия многоадресного маршрутизатора VLAN из-за того, что очередь сообщений заполнена.
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating small buffers	Не удалось распределить буферы для малых пакетов IGMP.
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating large buffers	Не удалось распределить буферы для крупных пакетов IGMP.

Сообщения журнала GARP/GVRP/GMRP

Компонент	Сообщение	Причина
GARP/GVRP/ GMRP	garpSpanState, garpIfStateChange, GarpIssueCmd, garpDot1sChangeCallBack, garpApiCnfgrCommand, garpLeaveAllTimerCallback, garpTimerCallback: QUEUE SEND FAILURE:	Очередь garpQueue заполнена, особенности сообщения (внутренний номер интерфейса, тип и т.д.) занесены в журнал.
GARP/GVRP/ GMRP	GarpSendPDU: QUEUE SEND FAILURE	Очередь garpPduQueue заполнена, особенности GPDU (внутренний номер интерфейса, vlan id, и т.д.) занесены в журнал.
GARP/GVRP/ GMRP	garpMapIntfIsConfigurable, gmrpMapIntfIsConfigurable: Error accessing GARP/GMRP config data for interface %d in garpMapIntfIsConfigurable.	Для этого интерфейса не существует конфигурации по умолчанию. Обычно по причине нового интерфейса, который не имеет предконфигурации.
GARP/GVRP/ GMRP	garpTraceMsgQueueUsage: garpQueue usage has exceeded fifty/eighty/ninety percent	Отслеживает построение очереди сообщений. Полезно при определении нагрузки на GARP.
GARP/GVRP/ GMRP	gid_destroy_port: Error Removing port %d registration for vlan-mac %d - %02X:%02X:%02X:%02X:%02X:%02X	Несовпадение между gmd (базой данных gmrp) и MFDB.
GARP/GVRP/ GMRP	gmd_create_entry: GMRP failure adding MFDB entry: vlan %d and address %s	Таблица MFDB заполена.

Сообщения журнала 802.3ad

Компонент	Сообщение Причина	
802.3ad	dot3adReceiveMachine: received default	Получен LAG PDU и машина состояний RX state event %x игнорирует данный LAGPDU.
802.3ad	dot3adNimEventCompletionCallback, dot3adNimEventCreateCompletion	Настроенное событие не завершено успешно.

Компонент	Сообщение Причина	
	Callback: DOT3AD: notification failed for event(%d), intf(%d), reason(%d)	

Сообщения журнала FDB

Компонент	Сообщение Причина	
FDB	fdbSetAddressAgingTimeOut: Failure setting fid %d address aging timeout to %d	Невозможно установить время устаревания на устройстве.

MFDB Log Message

Компонент	Сообщение	Причина
MFDB	mfdbTreeEntryUpdate: entry does not exist	Попытка обновления несуществующей записи.

Сообщения журнала 802.1Q

Компонент	Сообщение	Причина
802.1Q	dot1qIssueCmd: Unable to send message %d to dot1qMsgQueue for vlan %d - %d msgs in queue	Очередь dot1qMsgQueue заполнена.
802.1Q	dot1qVlanCreateProcess: Attempt to create a vlan with an invalid vlan id %d ; VLAN %d not in range.	Применяется для зарезервированных VLAN ID (4094 - x).
802.1Q	dot1qMapIntfIsConfigurable: Error accessing DOT1Q config data for interface %d in dot1qMapIntfIsConfigurable.	Для этого интерфейса не существует конфигурации по умолчанию. Как правило, это происходит тогда, когда новый интерфейс создан, но не имеет предварительно сохраненной конфигурации.
802.1Q	dot1qVlanDeleteProcess: Deleting the default VLAN	Как правило, выводится во время очищения Vlan и конфигурации.

Компонент	Сообщение	Причина
802.1Q	dot1qVlanMemberSetModify, dot1qVlanTaggedMemberSetModify: Dynamic entry %d can only be modified after it is converted to static	Если сведения об этой VLAN получены через GVRP, изменить ее набор членов через функцию управления не удается.
802.1Q	dtl failure when adding ports to vlan id %d - portMask = %s	Не удается аппаратно добавить порты к записи VLAN.
802.1Q	dtl failure when deleting ports from vlan id %d portMask = %s	Не удается аппаратно удалить порты из записи VLAN .
802.1Q	dtl failure when adding ports to tagged list for vlan id %d - portMask = %s	Не удается аппаратно добавить порты к тегированному списку VLAN ID.
802.1Q	dtl failure when deleting ports from tagged list for vlan id %d - portMask = %s	Не удается аппаратно удалить порты из тегированному списку VLAN ID.

Сообщения журнала 802.1Q (продолжение)

Компонент	Сообщение	Причина
802.1Q	dot1qTask: unsuccessful return code on receive from dot1qMsgQueue: %08x"	Не удается получить сообщение dot1q из очереди сообщений
802.1Q	Unable to apply VLAN creation request for VLAN ID %d, Database reached MAX VLAN count!	Не удается создать VLAN ID, база VLAN достигла предела своей емкости.
802.1Q	Attempt to create a vlan (%d) that already exists	Создание уже существующей динамической VLAN из командной строки
802.1Q	DTL call to create VLAN %d failed with rc %d"	Не удается аппаратно создать VLAN ID.
802.1Q	Problem unrolling data for VLAN %d	Не удалось удалить VLAN из базы данных VLAN после ошибки аппаратного создания VLAN.

Компонент	Сообщение	Причина
802.1Q	VLan %d does not exist	Не удается удалить запись VLAN.
802.1Q	VLan %d requestor type %d does not exist	Удалить динамический VLAN ID не удается, так как запрашивающая сторона недействительна.
802.1Q	Can not delete the VLAN, Some unknown component has taken the ownership!	Удаление не удается по причине передачи собственности неизвестному компоненту.
802.1Q	Not valid permission to delete the VLAN %d requestor %d	Не удается удалить VLAN ID, так как указанная запрашивающая сторона и состояние записи VLAN не совпадают.
802.1Q	VLAN Delete Call failed in driver for vlan %d	Не удается аппаратно удалить VLAN.
802.1Q	Problem deleting data for VLAN %d	Не удается удалить VLAN ID из базы данных VLAN.
802.1Q	Dynamic entry %d can only be modified after it is converted to static	Не удается модифицировать групповой фильтр VLAN.
802.1Q	Cannot find vlan %d to convert it to static	Не удаётся конвертировать динамическую VLAN в статическую. VLAN ID не существует.
802.1Q	Only Dynamically created VLANs can be converted	Не удаётся конвертировать созданную статическую VLAN в статическую.
802.1Q	Cannot modify tagging of interface %s to non existence vlan %d"	Ошибка при установке указанным интерфейсом свойства тегирования для всех VLAN в маске vlan.
802.1Q	Error in updating data for VLAN %d in VLAN database	Не удается добавить VLAN ID в базу данных VLAN.

Компонент	Сообщение	Причина
802.1Q	DTL call to create VLAN %d failed with rc %d	Не удается аппаратно добавить запись VLAN.
802.1Q	Not valid permission to delete the VLAN %d	Не удается удалить статический VLAN ID. Недействительный источник запроса.
802.1Q	Attempt to set access vlan with an invalid vlan id %d	Недействительный VLAN ID.
802.1Q	Attempt to set access vlan with (%d) that does not exist	VLAN ID не существует.
802.1Q	VLAN create currently underway for VLAN ID %d	Попытка создания VLAN, которая уже находится в процессе создания.
802.1Q	VLAN ID %d is already exists as static VLAN	Попытка создания уже существующего статического VLAN ID.
802.1Q	Cannot put a message on dot1q msg Queue, Returns:%d	Не удалось отправить сообщение Dot1q в очередь сообщений Dot1q
802.1Q	Invalid dot1q Interface: %s	Не удается добавить VLAN к члену порта.
802.1Q	Cannot set membership for user interface %s on management vlan %d	Не удается добавить VLAN к члену порта.
802.1Q	Incorrect tagmode for vlan tagging. tagmode: %d Interface: %s	Некорректный режим тегирования VLAN
802.1Q	Cannot set tagging for interface %d on non existent VLAN %d"	VLAN ID не существует.
802.1Q	Cannot set tagging for interface %d which is not a member of VLAN %d	Не удается настроить конфигурацию тегирования для интерфейса или диапазона VLAN.
802.1Q	VLAN create currently underway for VLAN ID	Попытка создания VLAN, которая уже находится в процессе создания.

Компонент	Сообщение	Причина
802.1Q	VLAN ID %d already exists	Попытка создания уже существующего VLAN ID.
802.1Q	Failed to delete, Default VLAN %d cannot be deleted	Попытка удаления VLAN ID по умолчанию.
802.1Q	Failed to delete, VLAN ID %d is not a static VLAN	Попытка удаления динамического VLAN ID из командной строки
802.1Q	Requestor %d attempted to release internal VLAN %d: owned by %d	-

Сообщения журнала 802.1S

Компонент	Сообщение	Причина
802.1S	dot1sIssueCmd: Dot1s Msg Queue is full!!!!Event: %u, on interface: %u, for instance: %u	Очередь сообщений заполнена.
802.1S	dot1sStateMachineRxBpdu(): Rcvd BPDU Discarded	Текущие условия не позволяют обработать данный BPDU (например, отключенный порт либо незаконченная обработка другого BPDU на этом же интерфейсе).
802.1S	dot1sBpduTransmit(): could not get a buffer	Переполнение системных буферов..

Сообщения журнала Port Mac Locking og Message

Компонент	Сообщение	Причина
Port Mac Locking	pmlMapIntfIsConfigurable: Error accessing . PML config data for interface %d in pmlMapIntfIsConfigurable	Конфигурации по умолчанию для этого интерфейса не существует.Как правило, это происходит тогда, когда новый интерфейс уже создан, но не имеет предварительно сохраненной конфигурации.

11.5. QoS

Сообщения журнала ACL

Компонент	Сообщение	Причина
ACL	Total number of ACL rules (x) exceeds max (y) on intf i.	Совокупность всех списков ACL, примененных к интерфейсу, требует большего количества правил, нежели поддерживает платформа.
ACL	ACL name, rule x: This rule is not being logged	Конфигурация ACL привела к тому, что требуется большее количество правил журналирования, чем поддерживает платформа. Указанное правило работает нормально, за исключением действий журналирования.
ACL	aclLogTask: error logging ACL rule trap for correlator number	Системе не удалось отправить SNMP trap для этого правила ACL, содержащего атрибут ведения журнала.
ACL	IP ACL number: Forced truncation of one or more rules during config migration	При обработке сохраненной конфигурации система обнаружила ACL с бóльшим количеством правил, чем поддерживается текущей версией. Это может произойти, когда код обновляется до версии, поддерживающей меньшее количество правил для ACL, чем предыдущая версия.

Сообщения журнала CoS

Компонент	Сообщение	Причина
COS	cosCnfgrInitPhase3Process: Unable to apply saved config -- using factory defaults	Компонент COS не смог применить сохраненную конфигурацию и был инициализирован с настройками по умолчанию.

11.6. Стекирование

Сообщения журнала EDB

Компонент	Сообщение	Причина
EDB	EDB Callback: Unit Join: num.	Юнит *num* был присоединен к стеку.

11.7. Технологии

Сообщения об ошибке Switch

Компонент	Сообщение	Причина
Switch	In hapiBroadSystemMacAddress call to 'bcm_l2_addr_add' - FAILED : x	Не удалось добавить L2 адрес в таблицу MAC-адресов. Такое может случиться в случае коллизии хеша, а также если таблица заполнена.
Switch	Failed installing mirror action - rest of the policy applied successfully	Заранее настроенный зеркалируемый порт не использовался в данной политике.
Switch	Policy x does not contain rule x	Правило не было добавлено в политику из-за несоответствия количеству правил для этой конкретной политики. Кроме того, сообщение может отображаться при изменении старого правила, когда старое правило не входит в политику.
Switch	ERROR: policy x, tmpPolicy x, size x, data x possible x x x x x x x	Проблема с установкой политики из-за дублирования хэша.
Switch	ACL x not found in internal table	Попытка удаления несуществующего ACL.
Switch	ACL internal table overflow	Попытка добавить ACL в заполненную таблицу.
Switch	In hapiBroadQosCosQueueConfig, Failed to configure minimum bandwidth. Available bandwidth x	Попытка настроить полосу пропускания на значения за пределами возможности этой полосы.

Компонент	Сообщение	Причина
Switch	USL: failed to put sync response on queue	Ответ на запрос синхронизации не был поставлен в очередь. Это может указывать на то, что предыдущий запрос синхронизации был получен после истечения времени ожидания.
Switch	USL: failed to sync ipmc table on unit = x	Либо произошла ошибка при перемещении, либо пакет был отклонен.
Switch	usl_task_ipmc_msg_send(): failed to send with x	Либо произошла ошибка при передаче, либо пакет был отклонен.
Switch	USL: No available entries in the STG table	Таблица Spanning Tree Group заполнена в USL.
Switch	USL: failed to sync stg table on unit = x	Не удалось синхронизировать устройство x из-за ошибки передачи либо по причине проблемы API на удаленном устройстве. Будет предпринята повторная попытка синхронизации.
Switch	USL: A Trunk doesn't exist in USL	Попытка модификации несуществующего Trunk.
Switch	USL: A Trunk being created by bcmx already existed in USL	Возможная проблема синхронизации между приложением, аппаратным уровнем и уровнем синхронизации
Switch	USL: A Trunk being destroyed doesn't exist in USL	Возможная проблема синхронизации между приложением, аппаратным уровнем и уровнем синхронизации

Компонент	Сообщение	Причина
Switch	USL: A Trunk being set doesn't exist in USL	Возможная проблема синхронизации между приложением, аппаратным уровнем и уровнем синхронизации
Switch	USL: failed to sync trunk table on unit = x	Не удалось синхронизировать юнит x из-за ошибки передачи либо по причине проблемы API на удаленном юните. Будет предпринята повторная попытка синхронизации.
Switch	USL: Mcast entry not found on a join	Возможная проблема синхронизации между приложением, аппаратным уровнем и уровнем синхронизации
Switch	USL: Mcast entry not found on a leave	Возможная проблема синхронизации между приложением, аппаратным уровнем и уровнем синхронизации
Switch	USL: failed to sync policy table on unit = x	Не удалось синхронизировать юнит x из-за ошибки передачи либо по причине проблемы API на удаленном юните. Будет предпринята повторная попытка синхронизации.
Switch	USL: failed to sync VLAN table on unit = x	Не удалось синхронизировать юнит x из-за ошибки передачи либо по причине проблемы API на удаленном юните. Будет предпринята повторная попытка синхронизации.
Switch	Invalid LAG id x	Возможная проблема синхронизации между драйвером BCM и HAPI.
Switch	Invalid uport calculated from the BCM uport bcmx_l2_addr->lport = x	Uport недействителен из драйвера BCM.

Компонент	Сообщение	Причина
Switch	Invalid USP calculated from the BCM uport\nbcmx_l2_addr->lport = x	USP не может быть вычислен исходя из информации о событии, полученной для драйвера BCM.
Switch	Unable to insert route R/P	Маршрут R с префиксом P не может быть вставлен в аппаратную таблицу маршрутизации. Будет предпринята повторная попытка.
Switch	Unable to Insert host H	Хост H не может быть вставлен в аппаратную таблицу хостов. Будет предпринята повторная попытка.
Switch	USL: failed to sync L3 Intf table on unit = x	Не удалось синхронизировать юнит x из-за ошибки передачи либо по причине проблемы API на удаленном юните. Будет предпринята повторная попытка синхронизации.
Switch	USL: failed to sync L3 Host table on unit = x	Не удалось синхронизировать юнит x из-за ошибки передачи либо по причине проблемы API на удаленном юните. Будет предпринята повторная попытка синхронизации.
Switch	USL: failed to sync L3 Route table on unit = x	Не удалось синхронизировать юнит x из-за ошибки передачи либо по причине проблемы API на удаленном юните. Будет предпринята повторная попытка синхронизации.
Switch	USL: failed to sync initiator table on unit = x	Не удалось синхронизировать юнит x из-за ошибки передачи либо по причине проблемы API на удаленном юните. Будет предпринята повторная попытка синхронизации.

Компонент	Сообщение	Причина
Switch	USL: failed to sync terminator table on unit = x	Не удалось синхронизировать юнит x из-за ошибки передачи либо по причине проблемы API на удаленном юните. Будет предпринята повторная попытка синхронизации.
Switch	USL: failed to sync ip-multicast table on unit = x	Не удалось синхронизировать юнит x из-за ошибки передачи либо по причине проблемы API на удаленном юните. Будет предпринята повторная попытка синхронизации.

11.8. Поддержка ОС

Сообщения журнала Linux BSP

Компонент	Сообщение	Причина
Linux BSP	rc = 10	Второе сообщение зарегистрировано при загрузке, сразу после Starting code… Журналируется всегда.

Сообщения журнала OSAPI Linux

Компонент	Сообщение	Причина
OSAPI Linux	osapiNetLinkNeighDump: could not open socket! - or – ipstkNdpFlush: could not open socket! – or – osapiNetlinkDumpOpen: unable to bind socket! errno = XX	Не удалось открыть сокет netlink. Убедитесь, что “ARP Daemon support” (CONFIG_ARPD) включено на уровне ядра Linux, если не используется референсный код ядра.
OSAPI Linux	ipstkNdpFlush: sending delete failed	Ошибка при запросе ядра на удаление записи таблицы соседей (некорректное сообщение).

Компонент	Сообщение	Причина
OSAPI Linux	unable to open /proc/net/ipv6/conf/default/ hop_limit	IPv6 MIB объект прочтен, но процедурный файл не смонтирован, или запущенное ядро не имеет поддержки IPV6.
OSAPI Linux	osapimRouteEntryAdd, errno XX adding 0xYY to ZZ – or – osapimRouteEntryDelete, errno XX deleting 0xYY from ZZ	Ошибка добавления или удаления маршрута IPv4 (указан в шестнадцатеричной системе как YY) , на интерфесе с Linux именем ZZ. Код ошибки можно увидеть в errno.h.
OSAPI Linux	l3intfAddRoute: Failed to Add Route – or – l3intfDeleteRoute: Failed to Delete Route	Ошибка добавления или удаления шлюза по умолчанию в таблицу маршрутизации ядра.
OSAPI Linux	osapiNetIfConfig: ioctl on XX failed: addr: 0xYY, err: ZZ – or – osapiNetIPSet: ioctl on XX failed: addr: 0x%YY	Ошибка при настройке IP-адреса (YY, в шестнадцатеричной системе) на интерфейсе с Linux именем XX, по причине того, что этого интерфейса не существует.
OSAPI Linux	ping: sendto error	Проблема при попытке отправить пакет эхо-запроса ICMP для команды ping. Возможно, маршрут к указанной стети отсутствует.
OSAPI Linux	Failed to Create Interface	Нехватка памяти при инициализации системы.
OSAPI Linux	TAP Unable to open XX	Файл /dev/tap отсутствует, либо, если не используется референсный код ядра, в ядре отсутствует поддержка универсального драйвера устройств TUN/TAP.
OSAPI Linux	Tap monitor task is spinning on select failures – then – Tap monitor select failed: XX	Проблемы чтения устройства /dev/tap, подробности в сообщении об ошибке XX.

Компонент	Сообщение	Причина
OSAPI Linux	Log_Init: log file error - creating new log file	Проблема с постоянным журналом событий в энергонезависимой памяти устройства. Либо его не существует, либо его контрольная сумма неверна.
OSAPI Linux	Log_Init: Flash (event) log full; erasing	Файл журнала был очищен. Это происходит во время загрузки.
OSAPI Linux	Log_Init: Corrupt event log; erasing	Файл журнала событий имеет непустую запись после пустой, что указывает на ошибку.
OSAPI Linux	Failed to Set Interface IP Address – or – IP Netmask – or – Broadcast Address – or – Flags – or – Hardware Address – or – Failed to Retrieve Interface Flags	Не удается добавить IP- или MAC-адрес(а) VRRP на сетевой интерфейс Linux.

12. АЛФАВИТНЫЙ УКАЗАТЕЛЬ КОМАНД

D

E

F

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

13. ОБЩАЯ ИНФОРМАЦИЯ

13.1. Замечания и предложения

Мы всегда стремимся улучшить нашу документацию и помочь вам работать лучше, поэтому мы хотим услышать вас. Мы всегда рады обратной связи, в особенности:

- ошибки в содержании, непонятные или противоречащие места в тексте;
- идеи по улучшению документации, чтобы находить информацию быстрее;
- неработающие ссылки и замечания к навигации по документу.

Если вы хотите написать нам по поводу данного документа, то используйте, пожалуйста, форму обратной связи на qtech.ru.

13.2. Гарантия и сервис

Процедура и необходимые действия по вопросам гарантии описаны на сайте QTECH в разделе «Поддержка» –> «Гарантийное обслуживание».

Ознакомиться с информацией по вопросам тестирования оборудования можно на сайте QTECH в разделе «Поддержка» –> «Взять оборудование на тест».

Вы можете написать напрямую в службу сервиса по электронной почте sc@qtech.ru.

13.3. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться нашей автоматизированной системой запросов технического сервис-центра helpdesk.qtech.ru.

Телефон Технической поддержки +7 (495) 797-33-11 доб. 0

13.4. Электронная версия документа

Дата публикации 21.06.2022

https://files.qtech.ru/upload/switchers/QSW-3750/QSW-3750_config_guide.pdf