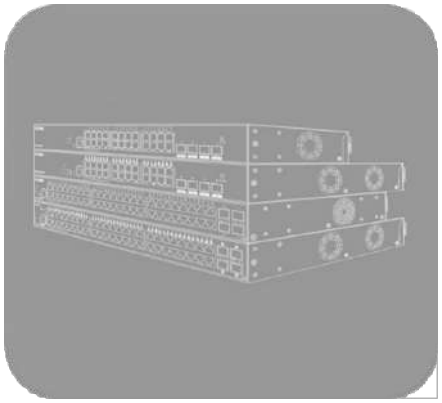


Руководство пользователя (CLI)

Серия DXS-1210
Настраиваемые 10-гигабитные коммутаторы

Версия 1.00

Содержание

1. Введение

Описание команд в данном руководстве основано на программном обеспечении версии **1.00**. Представленный здесь список является подмножеством команд, поддерживаемых коммутаторами серии DXS-1210.

Целевая аудитория

Руководство предназначено для сетевых администраторов и других IT-специалистов, использующих для управления коммутатором интерфейс командной строки (CLI). Это основной интерфейс управления настраиваемыми коммутаторами серии DXS-1210 (далее «коммутатор»). Настоящее руководство рассчитано на пользователей, знакомых с основными принципами работы Ethernet и организации современных локально-вычислительных сетей (ЛВС).

Прочая документация

Руководства, указанные ниже, являются дополнительным источником информации по настройке коммутатора и выявлению неисправностей. Документы доступны на веб-сайте D-Link:

- *Краткое руководство по установке коммутаторов серии DXS-1210*
- *Руководство пользователя по веб-интерфейсу коммутаторов серии DXS-1210*

Условные обозначения

Условное обозначение	Описание
Полужирный шрифт	Команды, опции команд и ключевые слова. Ключевые слова в командной строке необходимо вводить именно так, как они представлены в данном документе.
КУРСИВ ЗАГЛАВНЫМИ	Параметры или значения, которые необходимо указать. При вводе параметров в командной строке необходимо подставить фактические значения, для которых требуется выполнение данной команды.
Квадратные скобки [ ]	Дополнительное значение или набор дополнительных аргументов.
Фигурные скобки { }	Альтернативные ключевые слова заключаются в фигурные скобки и разделяются вертикальной чертой. Как правило, необходимо выбрать один из вариантов, разделенных вертикальной чертой.
Вертикальная черта |	Дополнительные значения или аргументы заключаются в квадратные скобки и разделяются вертикальной чертой. Как правило, необходимо указать одно или несколько значений/аргументов, разделенных вертикальной чертой.
`Цветной шрифт Courier`	Используется для иллюстрации работы с командной строкой, включая примеры команд с соответствующим выводом. Все примеры в данном руководстве основаны на работе с коммутатором DXS-1210-28T серии DXS-1210.

Предупреждения и примечания

При использовании данного руководства для управления коммутатором обращайте внимание на следующее:

Примечание: важная информация, которая может помочь в использовании устройства.

Внимание: информация о ситуациях, которые могут привести к повреждению устройства или потере данных, и способах их предотвращения.

Предупреждение: предупреждение о потенциальной опасности повреждения оборудования или угрозе для жизни и здоровья.

Подключение к консольному порту

Консольный порт используется для доступа к интерфейсу командной строки (CLI). Подключите консольный кабель (входит в комплект поставки) стороной с разъемом DB9 к последовательному (COM) порту компьютера и стороной с разъемом RJ45 к консольному порту коммутатора.

Для доступа к интерфейсу командной строки (CLI) через консольный порт необходимо использовать эмулятор терминала, например, PuTTY или Tera Term. При этом требуются скорость передачи данных **115200** бод, функция Flow Control должна быть выключена.

После завершения загрузки появится окно для входа CLI.

Описания команд

Информация о каждой команде в данном руководстве представлена с помощью следующих полей:

- **Описание** – краткое описание функционала команды.
- **Синтаксис** – точная форма команды и правила ее написания.
- **Параметры** – таблица с кратким описанием необязательных или обязательных для ввода параметров и их использованием в команде.
- **По умолчанию** – если команда задает новое значение конфигурации или административное состояние коммутатора, которые отличаются от настроек по умолчанию, то это указывается в данном поле.
- **Режим ввода команды** – режим, в котором возможно использование команды. Режимы описаны в разделе «Режимы ввода команд».
- **Использование команды** – детальное описание команды и различных сценариев ее использования.
- **Пример (-ы)** – пример использования команды в подходящем сценарии.

Режимы ввода команд

В интерфейсе командной строки (CLI) используется несколько режимов ввода команд. Набор доступных команд зависит от режима. Ввод вопросительного знака (**?**) после приглашения системы позволяет вывести список команд, доступных пользователю в определенном командном режиме.

В интерфейсе командной строки (CLI) доступно несколько режимов.
Базовые режимы:

EXEC Mode (Режим EXEC);

Global Configuration Mode (Режим глобальной конфигурации).

Переход в специальные режимы конфигурирования выполняется из режима **Global Configuration Mode.**

EXEC Mode (Режим EXEC)

Поддерживается контроль и управление всей информацией о системе и настройках. Пользователь также может просматривать и вносить любые изменения в настройки безопасности.

Global Configuration Mode (Режим глобальной конфигурации)

Данный режим позволяет вносить изменения в глобальные настройки всей системы. Помимо применения глобальных настроек для всей системы, данный режим также используется для перехода в специальные режимы конфигурирования. Для доступа к режиму глобальной конфигурации пользователь должен ввести команду **configure terminal** в режиме EXEC.

В следующем примере показано, как войти в режим Global Configuration.

```
Switch#configure terminal
Switch(config)#
```

Команда **exit** используется для выхода из режима глобальной конфигурации и возвращения в режим EXEC:

```
Switch(config)#exit
Switch#
```

Порядок действий для входа в специальные режимы конфигурирования представлен в дальнейших главах руководства. Данные командные режимы используются для конфигурирования отдельных функций.

Создание пользовательской учетной записи

Можно создать несколько учетных записей. Этот раздел поможет пользователю создать учетную запись с помощью интерфейса командной строки.

Примечание: по умолчанию на коммутаторе настроена одна учетная запись. Имя пользователя и пароль: admin.

Рассмотрим следующий пример:

```
Switch#configure terminal
Switch(config)#username account password account
```

В данном примере получен доступ к команде username.

- Используется команда **configure terminal** для перехода к глобальному режиму конфигурации. Данный режим позволяет использовать команду **username**.

- С помощью команды **username account password account** создается учетная запись пользователя с именем *account* и паролем *account.*

Сохраните текущую конфигурацию как конфигурацию запуска (start-up configuration), чтобы при перезагрузке коммутатора внесенные изменения не были утеряны. В следующем примере показано, как сохранить текущую конфигурацию в качестве конфигурации запуска:

```
Switch#copy running-config startup-config

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM..... Done.

Switch#
```

После перезагрузки коммутатора или выхода из учетной записи можно будет зайти в интерфейс командной строки с новым именем пользователя и паролем, как показано в примере ниже:

```
                DXS-1210-28T 10 Gigabit Ethernet Smart Managed Switch

                              Command Line Interface
                             Firmware: Build 1.00.021
           Copyright(C) 2020 D-Link Corporation. All rights reserved.

User Access Verification

Username:admin
Password:*****
```

Сообщения об ошибке

Если коммутатор не распознает введенную команду, появятся сообщения об ошибке с основной информацией о проблеме. В таблице ниже указаны возможные сообщения об ошибках с описанием проблемы.

Сообщение об ошибке	**Описание**
Ambiguous command	Введено недостаточно ключевых слов для распознавания команды.
Incomplete command	Введены не все ключевые слова, необходимые для выполнения команды.
Invalid input detected at ^marker	Команда введена некорректно.

В примере ниже показано, как генерируется сообщение об ошибке Ambiguous command.

```
Switch#show v
Ambiguous command
Switch#
```

В примере ниже показано, как генерируется сообщение об ошибке Incomplete command.

```
Switch#show
Incomplete command
Switch#
```

В примере ниже показано, как генерируется сообщение об ошибке Invalid input detected.

```
Switch#show verb
             ^
Invalid input detected at ^marker
Switch#
```

Функции редактирования

Интерфейс командной строки коммутатора поддерживает следующие клавиши для редактирования:

Клавиша	**Описание**
Delete	Удаляет символ справа от курсора и перемещает оставшуюся часть строки влево.
Backspace	Удаляет символ слева от курсора и перемещает оставшуюся часть строки влево.
Стрелка влево	Перемещает курсор влево.
Стрелка вправо	Перемещает курсор вправо.
CTRL+R	Включает и отключает функцию вставки текста. При включении текст можно вставить в строку, а оставшаяся часть текста будет перемещена вправо. При выключении текст можно вставить в строку, а предыдущий текст будет автоматически заменен новым.
Return	Прокручивает вниз к следующей строке или используется для ввода команды.
Пробел	Прокручивает вниз на следующую страницу.
ESC	Выход из отображаемой страницы.

Фильтрация результатов вывода команды show

Для фильтрации результатов вывода команды **show** используются следующие параметры:

- **begin** *FILTER-STRING* — данный параметр используется для отображения первой строки, которая совпадает со строкой фильтра;
- **include** *FILTER-STRING* — данный параметр используется для отображения всех строк, совпадающих со строкой фильтра;
- **exclude** *FILTER-STRING* — данный параметр используется для исключения всех строк, совпадающих со строкой фильтра.

В данном примере показано использование параметра **begin** *FILTER-STRING* в команде **show**.

```
Switch#show running-config | begin line console
line console
 session-timeout 0
!
line telnet
!
line ssh
!
interface Ethernet1/0/1
!
interface Ethernet1/0/2
!
interface Ethernet1/0/3
!
interface Ethernet1/0/4
!
interface Ethernet1/0/5
!
interface Ethernet1/0/6
!
interface Ethernet1/0/7
!
interface Ethernet1/0/8
!
interface Ethernet1/0/9
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

В следующем примере показано использование параметра **include** *FILTER-STRING* в команде **show**.

```
Switch#show running-config | include Firmware
!                           Firmware: Build 1.00.021


Switch#
```

В примере ниже показано использование параметра **exclude** *FILTER-STRING* в команде **show**.

```
Switch#show running-config | exclude !
Building configuration...

Current configuration : 1416 bytes


ip http timeout-policy idle 36000
line console
 session-timeout 0
line telnet
line ssh
interface Ethernet1/0/1
interface Ethernet1/0/2
interface Ethernet1/0/3
interface Ethernet1/0/4
interface Ethernet1/0/5
interface Ethernet1/0/6
interface Ethernet1/0/7
interface Ethernet1/0/8
interface Ethernet1/0/9
interface Ethernet1/0/10
interface Ethernet1/0/11
interface Ethernet1/0/12
interface Ethernet1/0/13
interface Ethernet1/0/14
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

2. Базовые команды интерфейса командной строки

2.1 help

Данная команда используется для отображения краткой справочной информации. Используйте команду **help** в любом режиме.

help

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Любой режим конфигурирования.

Использование команды

Команда **help** применяется для получения краткой справочной информации, включая следующее:

- Чтобы получить список команд для конкретного режима, после приглашения системы введите вопросительный знак (?).
- Чтобы получить список команд, начинающихся с определенной символьной строки, введите сокращенную команду и следующий за ней вопросительный знак (?). Такая форма справки называется справкой **по слову** (word help), так как в ней содержатся только ключевые слова или аргументы, начинающиеся с введенного сокращения.
- Чтобы получить список ключевых слов и аргументов для определенной команды, введите в командной строке вопросительный знак (?) вместо ключевого слова или аргумента. Такая форма справки называется справкой **по синтаксису** команды (command syntax help), так как она показывает возможные ключевые слова или аргументы на основании уже введенной команды, ключевых слов или аргументов.

Пример

В данном примере показано использование команды **help** для вывода краткого описания возможностей системы справки.

```
Switch#help

The switch CLI provides advanced help feature.
1. Help is available when you are ready to enter a command
   argument (e.g. 'show ?') and want to know each possible
   available options.
2. Help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input(e.g. 'show ve?'.).
   If nothing matches, the help list will be empty and you must backup
   until entering a '?' shows the available options.
3. For completing a partial command name could enter the abbreviated
   command name immediately followed by a <Tab> key.

Note:
Since the character '?' is used for help purpose, to enter
the character '?' in a string argument, press ctrl+v immediately
followed by the character '?'.

Switch#
```

В примере ниже показано использование справки **по слову** для отображения команд режима Privileged EXEC Mode, начинающихся с «re». Буквы, введенные перед вопросительным знаком (?), также отображаются на следующей строке, что позволяет пользователю продолжить ввод команды.

```
Switch#re?
reboot  renew  reset

Switch#re
```

В следующем примере показано использование справки **по синтаксису команды**, позволяющей получить недостающий аргумент для частично введенной команды **copy**. Символы, введенные перед вопросительным знаком (?), также отображаются на следующей строке, что позволяет пользователю продолжить ввод команды.

```
Switch#copy ?
  attack-log      Copy from attack log
  flash:          Copy from flash: file system
  log             Copy from log
  running-config  Copy from current system configuration
  startup-config  Copy from boot-up configuration
  tftp:           Copy from tftp: file system

Switch#copy
```

2.2 configure terminal

Данная команда используется для входа в режим глобальной конфигурации (Global Configuration Mode).

configure terminal

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для входа в режим глобальной конфигурации.

Пример

В данном примере показано, как войти в режим глобальной конфигурации.

```
Switch# configure terminal
Switch(config)#
```

2.3 login (EXEC)

Данная команда используется для настройки имени пользователя.

login

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для смены пользователя и входа в систему с новой учетной записью. Разрешено 3 попытки входа в интерфейс коммутатора. При использовании Telnet, если все попытки будут неудачными, пользователь вернется к приглашению на ввод команды. Если в течение 60 секунд не вводится никаких данных, сессия вернется в состояние выхода из учетной записи.

Пример

В данном примере показано, как войти в учетную запись с именем пользователя «user1».

```
Switch#login

Username: user1
Password: xxxxx

Switch#
```

2.4 logout

Данная команда используется для завершения активной сессии и выхода пользователя из системы.

logout

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для завершения активной сессии и выхода пользователя из системы.

Пример

В данном примере показано, как выйти из системы.

```
Switch#logout
```

2.5 end

Данная команда используется для выхода из текущего режима конфигурации и возвращения к высшему режиму в иерархии CLI, т. е. к режиму EXEC.

end

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Любой режим конфигурирования.

Использование команды

Данная команда используется для возвращения к высшему режиму в иерархии режимов CLI, независимо от текущего режима или подрежима конфигурирования.

Пример

В данном примере показано, как завершить сеанс работы в режиме конфигурирования интерфейса Interface Configuration Mode и вернуться в режим EXEC Mode.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#end
Switch#
```

2.6 exit

Данная команда используется для выхода из текущего режима конфигурирования и возвращения к предыдущему режиму. Если текущим режимом является EXEC Mode, выполнение команды **exit** позволит выйти из текущей сессии.

exit

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Любой режим конфигурирования.

Использование команды

Данная команда применяется для выхода из текущего режима конфигурирования и возвращения к предыдущему режиму. Если текущим режимом является User EXEC Mode или Privileged EXEC Mode, выполнение команды **exit** позволит выйти из текущей сессии.

Пример

В данном примере показано, как вернуться из режима конфигурирования интерфейса (Interface Configuration Mode) в режим глобальной конфигурации (Global Configuration Mode).

```
Switch#configure terminal
Switch(config) interface eth1/0/1
Switch(config-if)#exit
Switch(config)#
```

2.7 show history

Данная команда используется для просмотра списка команд, введенных в текущей сессии режима EXEC Mode.

show history

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Все введенные команды сохраняются в системе. Для повторного вызова сохраненной команды используется сочетание клавиш **CTRL**+**P** или клавиша **Вверх**. Буфер истории рассчитан на 20 команд.

Навигация по командам в истории выполняется следующими комбинациями клавиш:

- CTRL+P или клавиша Вверх – для повторного вызова команд из буфера истории, начиная с последних. Повторите нажатие для просмотра более ранних команд.
- CTRL+N или клавиша Вниз – для возврата к более поздним командам в буфере истории после повторного вызова команд с помощью клавиш CTRL+P или Вверх. Повторите нажатие для последовательного вызова более поздних команд.

Пример

В данном примере показан процесс вызова буфера истории.

```
Switch#show history

 help
 history

Switch#
```

2.8 show environment

Данная команда используется для отображения информации о состоянии вентиляторов, температуре и питании.

show environment [fan | power | temperature]

Параметры

fan	(Опционально.) Укажите для отображения подробной информации о состоянии вентиляторов.
power	(Опционально.) Укажите для отображения подробной информации о питании.
temperature	(Опционально.) Укажите для отображения подробной информации о температуре.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если параметры не заданы, будут отображаться все типы информации.

Пример

В данном примере показано, как отобразить информацию о состоянии вентиляторов, температуре и питании устройства.

```
Switch# show environment

Detail Temperature Status:
Temperature Descr/ID          Current/Threshold Range
------------------------------------------------------
Central Temperature/1         33C/11~79C
Status code: * temperature is out of threshold range

Detail Fan Status:
------------------------------------------------------------
Right Fan 1 (OK)     Right Fan 2 (OK)

Detail Power Status:
Power Module      Power Status
----------------  -------------
Power 1           In-operation

Switch#
```

Отображаемые параметры

Power Status	**In-operation**: источник питания работает корректно.
	Failed: ошибка в работе источника питания.
	Empty: источник питания не подключен.

2.9 show unit

Данная команда позволяет получить общую информацию по устройствам стека.

show unit

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения информации об устройствах стека.

Пример

В данном примере показано, как отобразить информацию об устройствах в стеке.

```
Switch#show unit

Model Descr: 24P 10GBASE-T with 4P 25G SFP28
Model Name: DXS-1210-28T
Serial-Number: DXS1210102030
Status: OK
Up Time: 0DT1H30M18S
DRAM      255264 K total,   206868 K used,    48396 K free
FLASH      64640 K total,    38596 K used,    26044 K free

Switch#
```

2.10 show cpu utilization

Данная команда позволяет получить информацию об использовании ЦПУ.

show cpu utilization

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения данных по загрузке центрального процессора с интервалами 5 секунд, 1 минута и 5 минут.

Пример

В данном примере показано, как получить информацию о загрузке процессора.

```
Switch#show cpu utilization

CPU Utilization

Five seconds -   3 %         One minute -   3 %         Five minutes -   4 %


Switch#
```

2.11 show version

Данная команда используется для отображения информации о версии коммутатора.

show version

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения информации о версии коммутатора.

Пример

В данном примере показано, как отобразить информацию о версии коммутатора.

```
Switch#show version

System MAC Address: F0-7D-68-12-10-01

  Module Name: DXS-1210-28T
  H/W: A1
  Runtime: 1.00.021

Switch#
```

2.12 snmp-server enable traps environment

Данная команда используется для включения отправки trap-сообщений о состоянии питания, температуре и работе вентиляторов. Чтобы отключить отправку trap-сообщений, воспользуйтесь формой **no** этой команды.

snmp-server enable traps environment [fan] [power] [temperature]

no snmp-server enable traps environment [fan | power | temperature]

Параметры

fan	(Опционально.) Укажите, чтобы включить/отключить отправку предупреждающих trap-сообщений о событиях (остановка вентилятора или восстановление работы вентилятора).
power	(Опционально.) Укажите, чтобы включить/отключить отправку предупреждающих trap-сообщений о событиях (отказ питания или восстановление питания).

temperature	(Опционально.) Укажите, чтобы включить/отключить отправку предупреждающих trap-сообщений о событиях (превышение пороговых значений температуры или восстановление температуры).

По умолчанию

По умолчанию поддержка trap-сообщений для всех параметров отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда применяется для включения/отключения отправки trap-сообщений о состоянии питания, температуре и работе вентиляторов. Если параметры не указаны, будет включена или отключена поддержка trap-сообщений для всех параметров.

Пример

В данном примере показано, как включить отправку trap-сообщений.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps environment
Switch(config)#
```

2.13 environment temperature threshold

Данная команда используется, чтобы настроить пороговые значения температур для срабатывания термодатчика. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

environment temperature threshold thermal [high *VALUE*] **[low** *VALUE*]
no environment temperature threshold thermal [high] [low]

Параметры

high	(Опционально.) Укажите верхнюю границу температуры в градусах Цельсия. Диапазон значений: от -100 до 200.
low	(Опционально.) Укажите нижнюю границу температуры в градусах Цельсия. Диапазон значений: от -100 до 200. Нижняя граница не может быть выше верхней границы.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить пороговые значения температуры, соответствующие корректному диапазону рабочих температур, определенных для датчика. Нижняя граница температурного диапазона не может быть выше верхней. Настроенный диапазон должен быть в пределах минимума и максимума разрешенных температур, определенных для датчика. При превышении заданного порога будет отправлено уведомление.

Пример

В данном примере показано, как настроить диапазон температур для термодатчика.

```
Switch# configure terminal
Switch(config)#environment temperature threshold thermal high 100 low 20
Switch(config)#
```

2.14 show memory utilization

Данная команда используется для отображения информации об использовании памяти.

show memory utilization

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения информации об использовании памяти коммутатора, включая DRAM и flash-память.

Пример

В данном примере показано, как отобразить информацию об использовании памяти.

```
Switch#show memory utilization

DRAM      255264 K total,   206868 K used,    48396 K free
FLASH      64640 K total,    38596 K used,    26044 K free

Switch#
```

3. Команды 802.1X

3.1 clear dot1x counters

Данная команда используется для сброса счетчиков 802.1X (диагностика, статистика и статистика сессии).

clear dot1x counters {all | interface *INTERFACE-ID* **[, | -]}**

Параметры

all	Укажите для сброса счетчиков 802.1X (диагностика, статистика и статистика сессии) на всех интерфейсах.
interface *INTERFACE-ID*	Укажите для сброса счетчиков 802.1X (диагностика, статистика и статистика сессии) на определенном интерфейсе. Допустимыми интерфейсами являются физические порты (включая тип, номер в стеке и номер порта).
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для сброса всех счетчиков 802.1X (диагностика, статистика и статистика сессии).

Пример

В данном примере показано, как сбросить все счетчики 802.1X (диагностика, статистика и статистика сессии) на интерфейсе Ethernet 1/0/1.

```
Switch#clear dot1x counters interface eth1/0/1
Switch#
```

3.2 dot1x control-direction

Данная команда используется для настройки типа трафика на порту как однонаправленного (in) или двунаправленного (both). Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

dot1x control-direction {both | in}

no dot1x control-direction

Параметры

both	Укажите для включения контроля трафика в двух направлениях.
in	Укажите для включения контроля трафика в одном направлении.

По умолчанию

По умолчанию используется двунаправленный режим.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта. Если управление портом настроено как **force-authorized**, то контроль трафика в обоих направлениях не осуществляется. Если управление портом настроено как **auto**, то для контроля трафика в заданном направлении необходимо пройти процедуру аутентификации. Если управление портом настроено как **force-unauthorized**, доступ к управлению направлением заблокирован.

Предположим, что управление портом настроено как **auto**. Если направление задано как **both**, порт может принимать и передавать только пакеты EAPOL. Весь пользовательский трафик заблокирован до аутентификации. Если направление задано как **in**, в дополнение к приему и передаче пакетов EAPOL, порт может передавать пользовательский трафик, но не может получать его до аутентификации. Направление **in** является действующим только при режиме **multi-host**, настроенном с использованием команды **authentication host-mode**.

Пример

В данном примере показано, как настроить контроль трафика на интерфейсе Ethernet 1/0/1 в качестве однонаправленного.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1x control-direction in
Switch(config-if)#
```

3.3 dot1x default

Данная команда применяется для возврата параметров IEEE 802.1X определенного порта к настройкам по умолчанию.

dot1x default

Параметры

Нет.

По умолчанию

Аутентификация IEEE 802.1X отключена.

Двунаправленный режим потока.
Управление портом – автоматическое.
Forward PDU на порту отключено.
Максимальное количество запросов – 2.
Таймер сервера – 30 секунд.
Таймер запроса – 30 секунд.
Интервал передачи – 30 секунд.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда используется для возврата параметров IEEE 802.1X определенного порта к настройкам по умолчанию.

Пример

В данном примере показано, как сбросить параметры IEEE 802.1X на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1x default
Switch(config-if)#
```

3.4 dot1x port-control

Данная команда используется для управления состоянием авторизации порта. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

dot1x port-control {auto | force-authorized | force-unauthorized}
no dot1x port-control

Параметры

auto	Укажите, чтобы включить аутентификацию IEEE 802.1X для порта.
force-authorized	Укажите, чтобы порт считался принудительно авторизованным.
force-unauthorized	Укажите, чтобы порт считался принудительно неавторизованным.

По умолчанию

Параметр по умолчанию – **auto.**

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.

Данная команда вступает в силу, только если аутентификатор IEEE 802.1X PAE глобально включен командой **dot1x system-auth-control** и включен для определенного порта с помощью режима аутентификатора dot1x PAE.

При выборе параметра **force-authorized** контроль трафика в обоих направлениях не осуществляется. При выборе параметра **auto** для контроля трафика в заданном направлении необходимо пройти процедуру аутентификации. При выборе параметра **force-unauthorized** управление портом в указанном направлении заблокировано.

Пример

В данном примере показано, как запретить доступ на интерфейс Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1x port-control force-unauthorized
Switch(config-if)#
```

3.5 dot1x forward-pdu

Данная команда используется для включения функции продвижения кадров dot1x PDU. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

dot1x forward-pdu

no dot1x forward-pdu

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта. Команда действует, только если аутентификация dot1x на настраиваемом порту отключена. Принятые PDU будут перенаправлены либо с тегом, либо без тега в зависимости от настроек VLAN.

Пример

В данном примере показано, как настроить продвижение кадров dot1x PDU.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1x forward-pdu
Switch(config-if)#
```

3.6 dot1x initialize

Данная команда используется для включения режима аутентификатора на определенном порту или ассоциированного с определенным MAC-адресом.

dot1x initialize {interface *INTERFACE-ID* **[, | -] | mac-address** *MAC-ADDRESS***}**

Параметры

interface *INTERFACE-ID*	Укажите порт, на котором будет инициирована аутентификация. Доступными интерфейсами являются физические порты.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
mac-address *MAC-ADDRESS*	Укажите MAC-адрес для инициализации.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

В режиме multi-host укажите ID интерфейса для инициализации определенного порта.

В режиме multi-auth укажите MAC-адрес для инициализации определенного MAC-адреса.

Пример

В данном примере показано, как инициализировать режим аутентификатора для интерфейса Ethernet 1/0/1.

```
Switch#dot1x initialize interface eth1/0/1
Switch#
```

3.7 dot1x max-req

Данная команда используется, чтобы задать максимальное количество попыток для передачи клиенту запроса EAP (Extensive Authentication Protocol) от внутреннего сервера аутентификации, прежде чем инициировать повторную аутентификацию. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

dot1x max-req *TIMES*

no dot1x max-req

Параметры

TIMES	Укажите количество запросов, в которых коммутатор повторно передает кадр EAP запрашивающему устройству перед перезапуском процесса аутентификации. Диапазон значений: от 1 до 10.

По умолчанию

По умолчанию используется значение 2.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта. Если клиент не отвечает на запрос аутентификации в течение периода, заданного командой **dot1x timeout tx-period** *SECONDS,* коммутатор отправит повторный запрос. Используйте команду, чтобы задать количество повторных попыток для передачи запроса.

Пример

В данном примере показано, как задать максимальное число попыток для передачи запроса на интерфейсе Ethernet 1/0/1. Указанное значение – 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1x max-req 3
Switch(config-if)#
```

3.8 dot1x pae authenticator

Данная команда используется для конфигурирования определенного порта в качестве аутентификатора IEEE 802.1X PAE (Port Access Entity). Чтобы отключить использование порта в качестве аутентификатора IEEE 802.1X, воспользуйтесь формой **no** этой команды.

dot1x pae authenticator
no dot1x pae authenticator

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта. Необходимо глобально включить аутентификацию IEEE 802.1X на коммутаторе с помощью команды **dot1x system-auth-control**. Если аутентификация IEEE 802.1X включена, система будет аутентифицировать пользователя 802.1X на основе списка методов, указанных командой **aaa authentication dot1x default**.

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 в качестве аутентификатора IEEE 802.1X PAE.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#
```

В примере ниже показано, как отключить аутентификацию IEEE 802.1X для интерфейса Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#no dot1x pae authenticator
Switch(config-if)#
```

3.9 dot1x re-authenticate

Данная команда используется для повторной аутентификации определенного порта или MAC-адреса.

dot1x re-authenticate {interface *INTERFACE-ID* **[, | -] | mac-address** *MAC-ADDRESS***}**

Параметры

interface *INTERFACE-ID*	Укажите порт для повторной аутентификации. Доступными интерфейсами являются физические порты.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
mac-address *MAC-ADDRESS*	Указание MAC-адреса для повторной аутентификации.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для повторной аутентификации определенного порта или MAC-адреса.

В режиме multi-host укажите ID интерфейса для повторной аутентификации определенного порта.
В режиме multi-auth укажите MAC-адрес для повторной аутентификации определенного MAC-адреса.

Пример

В данном примере показано, как включить повторную аутентификацию для интерфейса Ethernet 1/0/1.

```
Switch#dot1x re-authenticate interface eth1/0/1
Switch#
```

3.10 dot1x system-auth-control

Данная команда используется для глобального включения аутентификации IEEE 802.1X на коммутаторе. Чтобы отключить аутентификацию IEEE 802.1X, воспользуйтесь формой **no** этой команды.

dot1x system-auth-control
no dot1x system-auth-control

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

При включении функции аутентификации IEEE 802.1X неавторизованные узлы не смогут получать доступ к сети. Используйте команду **dot1x system-auth-control** для глобального включения аутентификации IEEE 802.1X. Если аутентификация IEEE 802.1X включена, система будет аутентифицировать пользователя 802.1X на основе списка методов, указанных командой **aaa authentication dot1x default**.

Пример

В данном примере показано, как включить аутентификацию IEEE 802.1X глобально на коммутаторе.

```
Switch#configure terminal
Switch(config)#dot1x system-auth-control
Switch(config)#
```

3.11 dot1x timeout

Данная команда используется для настройки таймеров IEEE 802.1X. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

dot1x timeout {server-timeout *SECONDS* **| supp-timeout** *SECONDS* **| tx-period** *SECONDS***}**
no dot1x timeout {server-timeout | supp-timeout | tx-period}

Параметры

server-timeout *SECONDS*	Укажите период времени в секундах, в течение которого коммутатор ожидает запрос от сервера аутентификации. По истечении времени ожидания аутентификатор отправит клиенту пакет EAP-Request. Диапазон значений: от 1 до 65535.
supp-timeout *SECONDS*	Укажите период времени в секундах, в течение которого коммутатор ожидает ответ от запрашивающего устройства. По истечении времени ожидания все сообщения от запрашивающего устройства, кроме запроса EAP request ID, будут недействительны. Диапазон значений от 1 до 65535.
tx-period *SECONDS*	Укажите период времени в секундах, в течение которого коммутатор ожидает ответ на запрос EAP-Request/Identity от клиента перед повторной отправкой запроса. Диапазон значений от 1 до 65535.

По умолчанию

Значение **server-timeout** по умолчанию составляет 30 секунд.

Значение **supp-timeout** по умолчанию составляет 30 секунд.

Значение **tx-period** по умолчанию составляет 30 секунд.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.

Пример

В данном примере показано, как задать на интерфейсе Ethernet 1/0/1 время ожидания ответа от сервера (15 секунд) и запрашивающего устройства (15 секунд), а также время ожидания перед повторной отправкой запроса клиенту (Tx-period =10 секунд).

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1x timeout server-timeout 15
Switch(config-if)#dot1x timeout supp-timeout 15
Switch(config-if)#dot1x timeout tx-period 10
Switch(config-if)#
```

3.12 show dot1x

Данная команда используется для отображения глобальной конфигурации IEEE 802.1X или конфигурации интерфейса.

show dot1x [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейс или группу интерфейсов, для которых будет отображаться конфигурация dot1x.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения глобальной конфигурации или конфигурации интерфейса. Если параметры не указаны, будет отображаться глобальная конфигурация.

Пример

В данном примере показано, как включить отображение глобальной конфигурации dot1X.

```
Switch#show dot1x

802.1X                  : Enabled
Trap State              : Enabled

Switch#
```

В примере ниже показано, как включить отображение конфигурации dot1X для интерфейса Ethernet 1/0/1.

```
Switch#show dot1x interface eth1/0/1


Interface          : eth1/0/1
PAE                : Authenticator
Control Direction  : Both
Port Control       : Auto
Tx Period          : 30    sec
Supp Timeout       : 30    sec
Server Timeout     : 30    sec
Max-req            : 2     times
Forward PDU        : Enabled

Switch#
```

3.13 show dot1x diagnostics

Данная команда используется для просмотра результатов диагностики IEEE 802.1X.

show dot1x diagnostics [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейс или группу интерфейсов, для которых будут отображаться данные диагностики dot1x.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения результатов диагностики IEEE 802.1X. Если значение не указано, будут отображаться данные для всех интерфейсов.

Пример

В данном примере показано, как вывести данные диагностики dot1X для интерфейса Ethernet 1/0/1.

```
Switch#show dot1x diagnostics interface eth1/0/1

eth1/0/1 dot1x diagnostic information are following:
EntersConnecting                    : 20
EAP-LogoffsWhileConnecting          : 0
EntersAuthenticating                : 0
SuccessesWhileAuthenticating        : 0
TimeoutsWhileAuthenticating         : 0
FailsWhileAuthenticating            : 0
ReauthsWhileAuthenticating          : 0
EAP-StartsWhileAuthenticating       : 0
EAP-LogoffsWhileAuthenticating      : 0
ReauthsWhileAuthenticated           : 0
EAP-StartsWhileAuthenticated        : 0
EAP-LogoffsWhileAuthenticated       : 0
BackendResponses                    : 0
BackendAccessChallenges             : 0
BackendOtherRequestsToSupplicant    : 0
BackendNonNakResponsesFromSupplicant : 0
BackendAuthSuccesses                : 0
BackendAuthFails                    : 0

Switch#
```

3.14 show dot1x statistics

Данная команда используется для просмотра статистики IEEE 802.1X.

show dot1x statistics [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейс или группу интерфейсов, для которых будет отображаться статистика dot1x.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения статистики IEEE 802.1X. Если значение не указано, отображается статистика для всех интерфейсов.

Пример

В данном примере показано, как отобразить статистику dot1X для интерфейса Ethernet 1/0/1.

```
Switch# show dot1x statistics interface eth1/0/1

eth1/0/1 dot1x statistics information:
EAPOL Frames RX                : 1
EAPOL Frames TX                : 4
EAPOL-Start Frames RX          : 0
EAPOL-Req/Id Frames TX         : 6
EAPOL-Logoff Frames RX         : 0
EAPOL-Req Frames TX            : 0
EAPOL-Resp/Id Frames RX        : 0
EAPOL-Resp Frames RX           : 0
Invalid EAPOL Frames RX        : 0
EAP-Length Error Frames RX     : 0
Last EAPOL Frame Version       : 0
Last EAPOL Frame Source        : 00-10-28-00-19-78

Switch#
```

3.15 show dot1x session-statistics

Данная команда используется для отображения статистики сессий IEEE 802.1X.

show dot1x session-statistics [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейс или группу интерфейсов, для которых будет отображаться статистика сессии dot1x.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для просмотра статистической информации по сессиям IEEE 802.1X. Если значение не указано, будет отображаться информация для всех интерфейсов.

Пример

В данном примере показано, как отобразить статистику по сессиям dot1X для интерфейса Ethernet 1/0/1.

```
Switch#show dot1x session-statistics interface eth1/0/1

Eth1/0/1 session statistic counters are following:
SessionOctetsRX                         : 0
SessionOctetsTX                         : 0
SessionFramesRX                         : 0
SessionFramesTX                         : 0
SessionId                               :
SessionAuthenticationMethod             : Remote Authentication Server
SessionTime                             : 0
SessionTerminateCause                   :SupplicantLogoff
SessionUserName                         :

Switch#
```

3.16 snmp-server enable traps dot1x

Данная команда используется, чтобы включить отправку SNMP-уведомлений для аутентификации 802.1X. Для отключения отправки SNMP-уведомлений воспользуйтесь формой **no** этой команды.

snmp-server enable traps dot1x

no snmp-server enable traps dot1x

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы включить/отключить отправку SNMP-уведомлений для аутентификации 802.1X

Пример

В данном примере показано, как включить отправку trap-сообщений для аутентификации 802.1X.

```
configure terminal
Switch(config)# snmp-server enable traps dot1x
Switch(config)#
```

4. Команды ACL (Список управления доступом)

4.1 access-list resequence

Данная команда используется для изменения нумерации записей в списке доступа. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

access-list resequence {*NAME* **|** *NUMBER* **}** *STARTING-SEQUENCE-NUMBER INCREMENT*
no access-list resequence

Параметры

NAME	Укажите имя конфигурируемого списка доступа. Максимальное количество символов – 32.
NUMBER	Укажите номер конфигурируемого списка доступа.
STARTING-SEQUENCE-NUMBER	Укажите начальное значение, в соответствии с которым будут перегруппированы записи в списке. Значение по умолчанию – 10. Диапазон значений: от 1 до 65535.
INCREMENT	Укажите шаг для присвоения порядковых номеров. Значение по умолчанию – 10. Например, если значение шага равно 5, а начальный номер – 20, то последующим записям будут присвоены номера 25, 30, 35, 40 и т. д. Диапазон значений: от 1 до 32.

По умолчанию

Начальный порядковый номер по умолчанию – 10.

Значение шага по умолчанию – 10.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная функция применяется для изменения нумерации записей для указанного списка доступа в соответствии с начальным номером из параметра *STARTING-SEQUENCE-NUMBER* и шагом, заданным с помощью параметра *INCREMENT*. Если сгенерированный порядковый номер превышает максимально допустимое значение, то существующая нумерация записей не изменится.

Если правило создано без указания определенного порядкового номера, он будет присвоен автоматически. Первой записи в списке присваивается начальный порядковый номер, а каждая новая запись получает последующий номер с учетом заданного шага и помещается в конец списка.

После изменения начального порядкового номера или значения шага порядковые номера всех предыдущих правил (включая правила, назначенные пользователем) будут изменены согласно новым настройкам.

Пример

В данном примере показано, как изменить нумерацию записей для списка доступа на основе IP-адресации с именем R&D.

```
Switch#show access-list ip R&D

Extended IP access list R&D(ID: 3552)
     10 permit tcp any 10.20.0.0 0.0.255.255
     20 permit tcp any host 10.100.1.2
     30 permit icmp any any

Switch#configure terminal
Switch(config)#ip access-list extended R&D
Switch(config-ip-ext-acl)#5 permit tcp any 10.30.0.0 0.0.255.255
Switch(config-ip-ext-acl)#end
Switch#show access-list ip R&D

Extended IP access list R&D(ID: 3552)
     5 permit tcp any 10.30.0.0 0.0.255.255
     10 permit tcp any 10.20.0.0 0.0.255.255
     20 permit tcp any host 10.100.1.2
     30 permit icmp any any

Switch#configure terminal
Switch(config)#access-list resequence R&D 1 2
Switch(config)#exit
Switch#show access-list ip R&D

     Extended IP access list R&D(ID: 3552)
     1 permit tcp any 10.30.0.0 0.0.255.255
     3 permit tcp any 10.20.0.0 0.0.255.255
     5 permit tcp any host 10.100.1.2
     7 permit icmp any any

Switch#
```

4.2 acl-hardware-counter

Данная команда используется, чтобы включить аппаратный счетчик ACL указанного списка доступа (access-list) для функций ограничения доступа (access group). Для отключения аппаратных счетчиков воспользуйтесь формой **no** этой команды.

acl-hardware-counter {access-group {*ACCESS-LIST-NAME* | *ACCESS-LIST-NUMBER***}**
no acl-hardware-counter {access-group {*ACCESS-LIST-NAME* **|** *ACCESS-LIST-NUMBER***}**

Параметры

access-group *ACCESS-LIST-NAME*	Укажите имя конфигурируемого списка доступа.
access-group *ACCESS-LIST-NUMBER*	Укажите номер конфигурируемого списка доступа.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Команда включает аппаратный счетчик ACL для всех портов, к которым применяется определенное имя или номер списка доступа. Подсчитывается количество пакетов, к которым применимо каждое правило.

Пример

В данном примере показано, как включить функцию аппаратного счетчика ACL.

```
configure terminal
Switch(config)# acl-hardware-counter access-group abc
Switch(config)#
```

4.3 clear acl-hardware-counter

Данная команда используется для сброса аппаратных счетчиков ACL.

clear acl-hardware-counter {access-group [*ACCESS-LIST-NAME* **|** *ACCESS-LIST-NUMBER***]**

Параметры

access-group	Укажите группу доступа, которую необходимо удалить.
ACCESS-LIST-NAME	(Опционально.) Укажите название списка доступа, который необходимо удалить.
ACCESS-LIST-NUMBER	(Опционально.) Укажите номер списка доступа, который необходимо удалить.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если параметры не указаны, данная команда обнулит аппаратные счетчики сразу для всех списков управления доступом (access-group hardware counters).

Пример

В данном примере показано, как сбросить аппаратные счетчики для заданного списка управления доступом.

```
Switch#clear acl-hardware-counter access-group abc
Switch#
```

4.4 ip access-group

Данная команда используется для указания списка доступа IP (IP access list), который будет применяться к интерфейсу. При использовании формы **no** команда удалит список доступа.

ip access-group {*NAME* **|** *NUMBER***} [in | out]**

no ip access-group [*NAME* **|** *NUMBER***] [in | out]**

Параметры

NAME	Укажите имя используемого списка доступа IP. Максимальное количество символов – 32.
NUMBER	Укажите номер используемого списка доступа IP.
in	(Опционально.) Укажите, чтобы список доступа IP применялся для проверки пакетов во входящем направлении. Если направление не указано, используется **in**.
out	(Опционально.) Укажите, чтобы список доступа IP применялся для проверки пакетов в исходящем направлении.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Если группа доступа IP (IP access group) на интерфейсе уже настроена, то команда, применяемая позже, заменит предыдущие настройки. К одному и тому же интерфейсу нельзя применить несколько списков доступа одинакового типа, при этом могут применяться списки доступа разных типов.

Привязка группы доступа (access group) к интерфейсу будет расходовать ресурсы коммутатора для записей фильтрации. Если для активации команды не хватает ресурсов, появится сообщение об ошибке. Число портов ограничено. Если применение команды исчерпает выбор доступных портов, появится сообщение об ошибке.

Пример

В данном примере показано, как настроить список доступа IP «Strict-Control» в качестве группы доступа IP для порта Ethernet 1/0/2.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#ip access-group Strict-Control

PROMPT: The remaining applicable IP related access entries are 1536, remaining range entries
are 32.
Switch(config-if)#
```

4.5 ip access-list

Данная команда используется для создания или изменения списка доступа IP (IP access list). При использовании команды произойдет вход в режим IP Access List Configuration Mode. Чтобы удалить список доступа IP, воспользуйтесь формой **no** этой команды.

ip access-list [extended] *NAME* **[***NUMBER***]**
no ip access-list [extended] {*NAME* **|** *NUMBER***}**

Параметры

extended	(Опционально.) Укажите для использования расширенного списка доступа IP (extended IP access list) и возможности применить больше опций фильтрации. Если параметр не указан, список доступа будет считаться стандартным.
NAME	Укажите имя списка доступа IP. Максимальное количество символов – 32. Первым символом должна быть буква.
NUMBER	Укажите ID-номер (ID number) списка доступа IP. Диапазон значений для стандартных списков доступа IP: от 1 до 1999; для расширенных списков доступа IP: от 2000 до 3999.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Указанное имя должно быть уникальным среди всех списков доступа. Все символы, используемые в имени, чувствительны к регистру. Если номер списка доступа не указан, автоматически будет назначен самый большой неиспользуемый номер.

Пример

В данном примере показано, как настроить расширенный список доступа IP с именем «Strict-Control» и список доступа IP с именем «pim-srcfilter».

```
Switch#configure terminal
Switch(config)#ip access-list extended Strict-Control
Switch(config-ip-ext-acl)#permit tcp any 10.20.0.0 0.0.255.255
Switch(config-ip-ext-acl)#exit
Switch(config)#ip access-list pim-srcfilter
Switch(config-ip-acl)#permit host 172.16.65.193 any
Switch(config-ip-acl)#
```

4.6 ipv6 access-group

Данная команда используется для назначения списка доступа IPv6 (IPv6 access list), который будет применяться к интерфейсу. Чтобы удалить список доступа IPv6, воспользуйтесь формой **no** этой команды.

ipv6 access-group {*NAME* **|** *NUMBER***} [in | out]**

no ipv6 access-group [*NAME* **|** *NUMBER***] [in | out]**

Параметры

NAME	Укажите имя используемого списка доступа IPv6. Максимальная длина – 32 символа.
NUMBER	Укажите номер используемого списка доступа IPv6.
in	(Опционально.) Укажите, чтобы список доступа IPv6 применялся для проверки пакетов во входящем направлении. Если направление не указано, используется **in**.
out	(Опционально.) Укажите, чтобы список доступа IPv6 применялся для проверки пакетов в исходящем направлении.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

К одному и тому же интерфейсу нельзя применить несколько списков доступа одинакового типа, при этом могут применяться списки доступа разных типов. Привязка группы доступа (access group) к интерфейсу будет расходовать ресурсы коммутатора для записей фильтрации. Если для активации команды не хватает ресурсов, появится сообщение об ошибке.

Число портов ограничено. Если применение команды исчерпает выбор доступных портов, появится сообщение об ошибке.

Пример

В данном примере показано, как применить список доступа IPv6 «ip6-control» в качестве группы доступа IP для интерфейса Ethernet 1/0/3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ipv6 access-group ip6-control in

PROMPT: The remaining applicable IPv6 related access entries are 511, remaining range entr
ies are 32.
Switch(config-if)#
```

4.7 ipv6 access-list

Данная команда используется для создания или изменения списка доступа IPv6 (IPv6 access list). При использовании команды произойдет вход в режим IPv6 Access List Configuration Mode. Чтобы удалить список доступа IPv6, воспользуйтесь формой **no** этой команды.

ipv6 access-list [extended] *NAME* **[***NUMBER***]**
no ipv6 access-list [extended] {*NAME* **|** *NUMBER***}**

Параметры

extended	(Опционально.) Укажите для использования расширенного списка доступа IPv6 и возможности применить больше опций фильтрации. Если параметр не указан, список доступа IPv6 будет считаться стандартным.
NAME	Укажите имя списка доступа IPv6. Максимальное количество символов – 32.
NUMBER	Укажите номер ID (ID number) списка доступа IPv6. Диапазон значений для стандартных списков доступа IPv6: от 11000 до 12999; для расширенных списков доступа IPv6: от 13000 до 14999.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Указанное имя должно быть уникальным среди всех списков доступа. Все символы, используемые в имени, чувствительны к регистру. Если номер списка доступа не указан, автоматически будет назначен самый большой неиспользуемый номер из диапазона номеров списков доступа IPv6.

Пример

В данном примере показано, как настроить расширенный список доступа IPv6 (IPv6 access list) под именем «ip6-control».

```
Switch#configure terminal
Switch(config)#ipv6 access-list extended ip6-control
Switch(config-ipv6-ext-acl)#permit tcp any 2002:f03::1/16
Switch(config-ipv6-ext-acl)#
```

В данном примере показано, как настроить стандартный список доступа IPv6 (IPv6 access list) под именем «ip6-std-control».

```
Switch#configure terminal
Switch(config)#ipv6 access-list ip6-std-control
Switch(config-ipv6-acl)#permit any fe80::101:1/54
Switch(config-ipv6-acl)#
```

4.8 list-remark

Данная команда используется для добавления комментариев к указанным спискам ACL. Для удаления комментариев воспользуйтесь формой **no** этой команды.

list-remark *TEXT*
no list-remark

Параметры

TEXT	Укажите текст комментария (не более 256 символов).

По умолчанию

Нет.

Режим ввода команды

Access-list Configuration Mode.

Использование команды

Команда доступна в режимах MAC, IP и IPv6 Configure Mode.

Пример

В данном примере показано, как добавить комментарий к списку доступа.

```
Switch#configure terminal
Switch(config)#ip access-list extended R&D
Switch(config-ip-ext-acl)#list-remark This access-list is used to match any IP packets from
the host 10.2.2.1.
Switch(config-ip-ext-acl)#end
Switch#show access-list ip

Extended IP access list R&D(ID: 3999)
  10 permit host 10.2.2.1 any
  This access-list is used to match any IP packets from the host 10.2.2.1.

Switch#
```

4.9 mac access-group

Данная команда используется для определения списка MAC-адресов, применяемого к интерфейсу. Чтобы удалить группу доступа с интерфейса, воспользуйтесь формой **no** этой команды.

mac access-group {*NAME* **|** *NUMBER***} [in | out]**
no mac access-group [*NAME* **|** *NUMBER***] [in | out]**

Параметры

NAME	Укажите имя используемого списка доступа на основе MAC.

NUMBER	Укажите номер используемого списка управления доступом на основе MAC.
in	(Опционально.) Укажите, чтобы список доступа на основе MAC применялся для проверки пакетов во входящем направлении. Если параметр не указан, используется значение **in**.
out	(Опционально.) Укажите, чтобы список доступа на основе MAC применялся для проверки пакетов в исходящем направлении.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Если группа доступа на базе MAC-адресации уже настроена на интерфейсе, следующая команда перезапишет предыдущие настройки. Группы доступа на основе MAC не проверяют IP-пакеты.

К одному и тому же интерфейсу нельзя применить несколько списков доступа одинакового типа, при этом могут применяться списки доступа различных типов.

Привязка группы доступа (access group) к интерфейсу будет расходовать ресурсы коммутатора для записей фильтрации. Если для активации команды не хватает ресурсов, появится сообщение об ошибке.

Пример

В данном примере показано, как применить список доступа на основе MAC «daily-profile» к интерфейсу Ethernet 1/0/4.

```
Switch#configure terminal
Switch(config)#interface eth1/0/4
Switch(config-if)#mac access-group daily-profile in

PROMPT: The remaining applicable MAC related access entries are 896, remaining range entri
es are 32.
Switch(config-if)#
```

4.10 mac access-list

Данная команда используется для создания или изменения списков управления доступом на базе MAC-адресации. Команда позволяет войти в режим MAC Access List Configuration Mode. Чтобы удалить список управления доступом MAC, воспользуйтесь формой **no** этой команды.

mac access-list extended *NAME* **[***NUMBER***]**
no mac access-list extended {*NAME* **|** *NUMBER***}**

Параметры

NAME	Укажите имя списка управления доступом MAC (MAC access list). Максимальное количество символов – 32.
NUMBER	Укажите номер ID (ID number) списка управления доступом на основе MAC. Диапазон значений для расширенных списков доступа MAC: от 6000 до 7999.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы войти в режим MAC Access-list Configuration Mode, и введите команду **permit** или **deny**, чтобы указать правила. Указанное имя должно быть уникальным среди всех списков доступа. Имя чувствительно к регистру. Если номер списка доступа не задан, автоматически будет назначен самый большой неиспользуемый номер из диапазона номеров списков доступа на основе MAC.

Пример

В данном примере показано, как войти в режим MAC Access List Configuration Mode для списка доступа на основе MAC под именем «daily-profile».

```
Switch#configure terminal
Switch(config)#mac access-list extended daily-profile
Switch(config-mac-ext-acl)#
```

4.11 permit | deny (ip access-list)

Данная команда используется для добавления записи permit или deny. Чтобы удалить запись, воспользуйтесь формой **no** этой команды.

Расширенный список управления доступом (Extended Access List):

[*SEQUENCE-NUMBER***] {permit | deny} tcp {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK*] **{any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK*] **[***TCP-FLAG***] [[precedence** *PRECEDENCE* **[***MASK***]] [tos TOS [***MASK***]] | dscp** *DSCP* **[MASK]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} udp {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK*] **{any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK*] **[[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} icmp {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD***} {any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***} [***ICMP-TYPE [ICMP-CODE***] |**

ICMP-MESSAGE] **[[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} {gre | esp | eigrp | igmp | ipinip | ospf | pcp | pim | vrrp | protocol-id** *PROTOCOL-ID* **[***MASK***]} {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD***} {any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***} [fragments] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD***} [any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***] [fragments] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

Стандартный список доступа IP (Standard IP Access List):

[*SEQUENCE-NUMBER***] {permit | deny} {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD***} [any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***] [time-range** *PROFILE-NAME]*

no *SEQUENCE-NUMBER*

Параметры

SEQUENCE-NUMBER	Укажите порядковый номер. Диапазон значений: от 1 до 65535. Чем меньше номер, тем выше приоритет правила permit/deny.
any	Укажите для использования любого IP-адреса источника или IP-адреса назначения.
host *SRC-IP-ADDR*	Укажите определенный IP-адрес узла источника.
SRC-IP-ADDR SRC-IP-WILDCARD	Укажите группу IP-адресов источника, используя значение битовой маски (wildcard). Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
host *DST-IP-ADDR*	Укажите определенный IP-адрес узла назначения.
DST-IP-ADDR DST-IP-WILDCARD	Укажите группу IP-адресов назначения, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
precedence *PRECEDENCE*	(Опционально.) Укажите, чтобы пакеты могли фильтроваться по уровню приоритета (precedence). Доступны значения от 0 до 7.
MASK	(Опционально.) Укажите маску приоритета (precedence mask) (0x0-0x7). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
dscp *DSCP*	(Опционально.) Укажите DSCP-код для совпадений с заголовком IP. Диапазон значений: от 0 до 63 или выбор из следующих имен DSCP: af11 - 001010, af12 - 001100, af13 - 001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 - 110000, cs7 - 111000, default - 000000, ef - 101110.

MASK	(Опционально.) Укажите маску DSCP (0x0-0x3f). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
tos *TOS*	(Опционально.) Укажите, чтобы пакеты могли фильтроваться по уровню type of service. Доступны значения от 0 до 15.
MASK	(Опционально.) Укажите маску ToS (0x0-0xf). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
lt *PORT*	(Опционально.) Укажите для сопоставления, если значение порта меньше указанного.
gt *PORT*	(Опционально.) Укажите для сопоставления, если значение порта больше указанного.
eq *PORT*	(Опционально.) Укажите для сопоставления, если значение порта равно указанному.
neq *PORT*	(Опционально.) Укажите для сопоставления, если значение порта не равно указанному.
range *MIN-PORT MAX-PORT*	(Опционально.) Укажите для сопоставления, если значение попадает в указанный диапазон портов.
mask *PORT MASK*	(Опционально.) Укажите для сопоставления с портами, определенными маской. Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
TCP-FLAG	(Опционально.) Укажите поля TCP flag и указанные биты заголовка TCP с именем **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize) или **urg** (urgent).
fragments	(Опционально.) Укажите для фильтрации фрагментов пакета.
time-range *PROFILE-NAME*	(Опционально.) Укажите имя профиля временного интервала time-range, связанного со списком доступа и определяющего период его активации.
tcp, udp, icmp, igmp, ipinip, gre, esp, eigrp, ospf, pcp, pim, vrrp	Укажите протоколы 4 уровня.
PROTOCOL-ID	(Опционально.) Укажите Protocol ID. Диапазон значений: от 0 до 255.
MASK	(Опционально.) Укажите маску protocol ID (0x0-0xff). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
ICMP-TYPE	(Опционально.) Укажите тип сообщения ICMP. Доступны номера для типа сообщений от 0 до 255.

ICMP-CODE	(Опционально.) Укажите код сообщения ICMP. Доступны номера для кода сообщений от 0 до 255.
ICMP-MESSAGE	(Опционально.) Укажите сообщение ICMP. Для выбора доступны следующие предустановленные параметры: administratively-prohibited, alternate-address, conversion-error, host-prohibited, net-prohibited, echo, echo-reply, pointer-indicates-error, host-isolated, host-precedence-violation, host-redirect, host-tos-redirect, host-tos-unreachable, host-unknown, host-unreachable, information-reply, information-request, mask-reply, mask-request, mobile-redirect, net-redirect, net-tos-redirect, net-tos-unreachable, net-unreachable, net-unknown, bad-length, option-missing, packet-fragment, parameter-problem, port-unreachable, precedence-cutoff, protocol-unreachable, reassembly-timeout, redirect-message,r outer-advertisement, router-solicitation, source-quench, source-route-failed, time-exceeded, timestamp-reply, timestamp-request, traceroute, ttl-expired, unreachable.

По умолчанию

Нет.

Режим ввода команды

IP Access-list Configuration Mode.

Использование команды

Если правило создано без указания определенного порядкового номера, он будет присвоен автоматически. Первой записи в списке присваивается начальный порядковый номер 10, а каждая новая запись получает последующий номер с шагом 10 (т. е. 20, 30, 40 и т.д.) и помещается в конец списка.

С помощью команды **access-list resequence** можно изменить начальный порядковый номер и значение шага для нумерации в указанном списке доступа. После применения команды новым записям без присвоенного порядкового номера будет задан номер в соответствии с новыми настройками указанного списка доступа.

При назначении порядкового номера вручную рекомендуется заранее зарезервировать интервал значений на случай создания новых записей с меньшим порядковым номером. В противном случае добавить запись с меньшим порядковым номером будет сложно.

Порядковый номер должен быть уникальным в домене списка доступа. Если заданный порядковый номер уже занят, появится сообщение об ошибке.

При создании правила сопоставления для стандартного списка доступа IP (IP standard access list) указываются только поля IP-адреса источника и назначения.

Диапазон VLAN и диапазон портов TCP/UDP можно присвоить только на входном порту.

Пример

В данном примере показано, как создать 4 записи для расширенного списка доступа IP с названием «Strict-Control». Это следующие записи: разрешить TCP-пакеты для сети 10.20.0.0, разрешить TCP-пакеты для узла 10.100.1.2, разрешить все TCP-пакеты для порта назначения TCP 80 и разрешить все ICMP-пакеты.

```
Switch#configure terminal
Switch(config)#ip access-list extended Strict-Control
Switch(config-ip-ext-acl)#permit tcp any 10.20.0.0 0.0.255.255
Switch(config-ip-ext-acl)#permit tcp any host 10.100.1.2
Switch(config-ip-ext-acl)#permit tcp any any eq 80
Switch(config-ip-ext-acl)#permit icmp any any
Switch(config-ip-ext-acl)#
```

В следующем примере показано, как создать 2 записи для стандартного списка доступа IP с названием «std-acl». Это следующие записи: разрешить IP-пакеты для сети 10.20.0.0, разрешить IP-пакеты для узла 10.100.1.2.

```
Switch#configure terminal
Switch(config)#ip access-list std-acl
Switch(config-ip-acl)#permit any 10.20.0.0 0.0.255.255
Switch(config-ip-acl)#permit any host 10.100.1.2
Switch(config-ip-acl)#
```

4.12 permit | deny (ipv6 access-list)

Данная команда используется для добавления записи permit или deny в список доступа IPv6. При использовании формы **no** команда удалит запись из списка доступа IPv6.

Расширенный список доступа IPv6 (Extended IPv6 Access List):

[*SEQUENCE-NUMBER***] {permit | deny} tcp {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDR/PREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDR/PREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] [***TCP-FLAG***] [dscp** *VALUE* **[***MASK***] | traffic-class** *VALUE* **[***MASK***]] [flow-label** *FLOW-LABEL* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} udp {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDR/PREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDR/PREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] [dscp** *VALUE* **[***MASK***] | traffic-class** *VALUE* **[***MASK***]] [flow-label** *FLOW-LABEL* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} icmp {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDR/PREFIX-LENGTH***} {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDR/PREFIX-LENGTH***} [***ICMP-TYPE** *[ICMP-CODE***] |** *ICMP-MESSAGE***] [dscp** *VALUE* **[***MASK***] | traffic-class** *VALUE* **[***MASK***]] [flow-label** *FLOW-LABEL* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} {esp | pcp | sctp | protocol-id** *PROTOCOL-ID* **[***MASK***]} {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDR/PREFIX-LENGTH***} {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDR/PREFIX-LENGTH***} [fragments] [dscp** *VALUE* **[***MASK***] | traffic-class** *VALUE* **[***MASK***]] [flow-label** *FLOW-LABEL* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDR/PREFIX-LENGTH***} [any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDR/PREFIX-LENGTH***] [fragments] [dscp** *VALUE* **[***MASK***] | traffic-class** *VALUE* **[***MASK***]] [flow-label** *FLOW-LABEL* **[***MASK***]] [time-range** *PROFILE-NAME***]**

Стандартный список доступа IPv6 (Standard IPv6 Access List):

[*SEQUENCE-NUMBER***] {permit | deny} {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDR/PREFIX-LENGTH***} [any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDR/PREFIX-LENGTH***] [time-range** *PROFILE-NAME***]**

no *SEQUENCE-NUMBER*

Параметры

SEQUENCE-NUMBER	Укажите порядковый номер. Диапазон значений: от 1 до 65535. Чем меньше номер, тем выше приоритет правила permit/deny.
any	Укажите для использования любого IPv6-адреса источника или IPv6-адреса назначения.
host *SRC-IPv6-ADDR*	Укажите определенный IPv6-адрес узла источника.
SRC-IPV6-ADDR/PREFIX-LENGTH	Укажите IPv6-адрес сети источника.
host *DST-IPV6-ADDR*	Укажите определенный IPv6-адрес узла назначения.
DST-IPV6-ADDR/PREFIX-LENGTH	Укажите IPv6-адрес сети назначения.
tcp, udp, icmp, esp, pcp ,sctp	Укажите тип протокола 4 уровня.
dscp *VALUE*	(Опционально.) Укажите совпадающее значение класса трафика в заголовке IPv6. Диапазон значений: от 0 до 63 или следующие DSCP-имена: af11 - 001010, af12 - 001100, af13 - 001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 - 110000, cs7 - 111000, default (по умолчанию) - 000000, ef – 101110.
MASK	(Опционально.) Укажите маску DSCP (0x0-0x3f). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
traffic-class *VALUE*	(Опционально.) Укажите значение совпадающего класса трафика в заголовке IPv6. Диапазон значений: от 0 до 255.
MASK	(Опционально.) Укажите маску класса трафика (0x0-0xff). Если значение не указано, используется 0xff.
lt *PORT*	(Опционально.) Укажите для сопоставления, если значение порта меньше указанного.
gt *PORT*	(Опционально.) Укажите для сопоставления, если значение порта больше указанного.
eq *PORT*	(Опционально.) Укажите для сопоставления, если значение порта равно указанному.
neq *PORT*	(Опционально.) Укажите для сопоставления, если значение порта не равно указанному.

range *MIN-PORT MAX-PORT*	(Опционально.) Укажите для сопоставления, если значение попадает в указанный диапазон портов.
mask *PORT MASK*	(Опционально.) Укажите для сопоставления с портами, определенными маской. Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
PROTOCOL-ID	(Опционально.) Укажите Protocol ID. Диапазон значений: от 0 до 255.
MASK	(Опционально.) Укажите маску Protocol ID (0x0-0xff). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
ICMP-TYPE	(Опционально.) Укажите тип сообщения ICMP. Доступны номера типа сообщений от 0 до 255.
ICMP-CODE	(Опционально) Укажите код сообщения ICMP. Доступны номера кода сообщений от 0 до 255.
ICMP-MESSAGE	(Опционально.) Укажите сообщение ICMP. Для выбора доступны следующие предустановленные параметры: beyond-scope, destination-unreachable, echo-reply, echo-request, erroneous_header, hop-limit, multicast-listener-query, multicast-listener-done, multicast-listener-report, nd-na, nd-ns, next-header, no-admin, no-route, packet-too-big, parameter-option, parameter-problem, port-unreachable, reassembly-timeout, redirect, renum-command, renum-result, renum-seq-number, router-advertisement, router-renumbering, router-solicitation, time-exceeded, unreachable.
TCP-FLAG	(Опционально.) Укажите поля TCP flag и указанные биты заголовка TCP с именем **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize) или **urg** (urgent).
flow-label *FLOW-LABEL*	(Опционально.) Укажите значение flow label. Диапазон значений: от 0 до 1048575.
MASK	(Опционально.) Укажите маску flow label (0x0-0xfffff). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться. Если значение не указано, используется 0xfffff.
fragments	(Опционально.) Укажите для фильтрации фрагментов пакета.
time-range *PROFILE-NAME*	(Опционально.) Укажите имя профиля временного интервала, связанного со списком доступа и определяющего период его активации.

По умолчанию

Нет.

Режим ввода команды

MAC Access-list Configuration Mode.

Использование команды

Если правило создано без указания определенного порядкового номера, он будет присвоен автоматически. Первой записи в списке присваивается начальный порядковый номер 10, а каждая новая запись получает последующий номер с шагом 10 (т. е. 20, 30, 40 и т.д.) и помещается в конец списка.

С помощью команды **access-list sequence** можно изменить начальный порядковый номер и значение шага для нумерации записей в указанном списке доступа. После применения команды новым записям без присвоенного порядкового номера будет задана последовательность в соответствии с новыми настройками указанного списка доступа.

При назначении порядкового номера вручную рекомендуется заранее зарезервировать интервал значений на случай создания новых записей с меньшим порядковым номером. В противном случае добавить запись с меньшим порядковым номером будет сложно.

Порядковый номер должен быть уникальным в домене списка доступа. Если заданный порядковый номер уже занят, появится сообщение об ошибке.

Диапазон VLAN и диапазон портов TCP/UDP можно присвоить только на входном порту.

Пример

В данном примере показано, как создать 4 записи для расширенного списка доступа IPv6 с именем «ipv6-control». Это следующие записи: разрешить TCP-пакеты для сети ff02::0:2/16, разрешить TCP-пакеты для узла ff02::1:2, разрешить все TCP-пакеты для порта назначения TCP 80 и разрешить все ICMP-пакеты.

```
Switch#configure terminal
Switch(config)#ipv6 access-list extended ipv6-control
Switch(config-ipv6-ext-acl)#permit tcp any ff02::0:2/16
Switch(config-ipv6-ext-acl)#permit tcp any host ff02::1:2
Switch(config-ipv6-ext-acl)#permit tcp any any eq 80
Switch(config-ipv6-ext-acl)#permit icmp any any
Switch(config-ipv6-ext-acl)#
```

В примере ниже показано, как создать 2 записи для стандартного списка доступа IPv6 с именем «ipv6-std-control». Это следующие записи: разрешить IP-пакеты для сети ff02::0:2/16, разрешить IP-пакеты для узла ff02::1:2.

```
Switch#configure terminal
Switch(config)#ipv6 access-list ipv6-std-control
Switch(config-ipv6-acl)#permit any ff02::0:2/16
Switch(config-ipv6-acl)#permit any host ff02::1:2
Switch(config-ipv6-acl)#
```

4.13 permit | deny (mac access-list)

Данная команда используется для назначения правила, которое будет разрешать или запрещать продвижение пакетов. Чтобы удалить запись, воспользуйтесь формой **no** этой команды.

[*SEQUENCE-NUMBER***] {permit | deny } {any | host SRC-MAC-ADDR |** *SRC-MAC-ADDR SRC-MAC-WILDCARD***} {any | host** *DST-MAC-ADDR* **|** *DST-MAC-ADDR DST-MAC-WILDCARD***} [ethernet-type** *TYPEMASK* **[cos** *VALUE* **[***MASK***]] [{vlan** *VLAN-ID* **[***MASK***] | vlan-range** *MIN-VID MAX-VID***}] [time-range** *PROFILE-NAME***]**

no *SEQUENCE-NUMBER*

Параметры

SEQUENCE-NUMBER	Укажите порядковый номер. Диапазон значений: от 1 до 65535. Чем меньше номер, тем выше приоритет правила permit/deny.
any	Укажите для использования любого MAC-адреса источника или MAC-адреса назначения.
host *SRC-MAC-ADDR*	Укажите определенный MAC-адрес узла источника.
SRC-MAC-ADDR SRC-MAC-WILDCARD	Укажите группу MAC-адресов источника, используя значение битовой маски (wildcard). Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
host *DST-MAC-ADDR*	Укажите определенный MAC-адрес узла назначения.
DST-MAC-ADDR DST-MAC-WILDCARD	Укажите группу MAC-адресов назначения, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
ethernet-type *TYPE MASK*	(Опционально.) Укажите Ethernet-тип фильтруемых пакетов в виде шестнадцатеричного числа с диапазоном значений от 0 до FFFF или используйте имя типа Ethernet. Доступны следующие имена: aarp, appletalk, decnet-iv, etype-6000, etype-8042, lat, lavc-sca, mop-console, mop-dump, vines-echo, vines-ip, xns-idp или arp.
cos *VALUE*	(Опционально.) Укажите значение приоритета от 0 до 7.
MASK	(Опционально.) Укажите маску внешнего приоритета (outer priority mask) (0x0-0x7). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться. Если значение не указано, используется 0x7.
vlan *VLAN-ID*	(Опционально.) Укажите VLAN ID.
MASK	(Опционально.) Укажите маску outer VLAN ID (0x0-0x0fff). Если значение не указано, используется 0x0fff.
vlan-range *MIN-VID MAX-VID*	(Опционально.) Укажите диапазон VLAN, задав минимальное и максимальное значение VLAN ID.
time-range *PROFILE-NAME*	(Опционально.) Укажите имя профиля временного интервала, связанного со списком доступа и определяющего период его активации.

По умолчанию

Нет.

Режим ввода команды

MAC Access-list Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если правило создано без указания определенного порядкового номера, он будет присвоен автоматически. Первой записи в списке присваивается начальный порядковый номер 10, а каждая новая запись получает последующий номер с шагом 10 (т. е. 20, 30, 40 и т.д.) и помещается в конец списка.

С помощью команды **access-list sequence** можно изменить начальный порядковый номер и значение шага для нумерации записей в указанном списке доступа. После применения команды новым записям без присвоенного порядкового номера будет задан номер в соответствии с новыми настройками для указанного списка доступа.

При назначении порядкового номера вручную рекомендуется заранее зарезервировать интервал значений на случай создания новых записей с меньшим порядковым номером. В противном случае добавить запись с меньшим порядковым номером будет сложно.

Порядковый номер должен быть уникальным в домене списка доступа. Если заданный порядковый номер уже занят, появится сообщение об ошибке.

Диапазон VLAN можно присвоить только на входном порту.

В список может быть добавлено несколько записей. Для одних можно настроить разрешающее правило (permit), а для других – запрещающее (deny). Команды permit и deny могут соответствовать различным полям, доступным при настройке.

Пример

В данном примере показано, как настроить записи MAC в профиле daily-profile, чтобы разрешить доступ двум спискам MAC-адресов источника.

```
Switch#configure terminal
Switch(config)#mac access-list extended daily-profile
Switch(config-mac-ext-acl)#permit 00:80:33:00:00:00  00:00:00:ff:ff:ff any
Switch(config-mac-ext-acl)#permit 00:f4:57:00:00:00 00:00:00:ff:ff:ff any
Switch(config-mac-ext-acl)#
```

4.14 show access-group

Данная команда используется для просмотра информации о группах доступа (access group) для одного или нескольких интерфейсов.

show access-group [interface *INTERFACE-ID***]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите необходимый интерфейс.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если интерфейс не указан, будет отображаться информация обо всех интерфейсах.

Пример

В данном примере показано, как включить отображение списков доступа, применяемых ко всем интерфейсам.

```
Switch#show access-group

eth1/0/1:
  Inbound mac access-list : simple-mac-acl(ID: 7998)
  Inbound ip access-list  : simple-ip-acl(ID: 1998)

Switch#
```

4.15 show access-list

Данная команда используется для отображения информации о настройках списка доступа.

show access-list [ip [*NAME* **|** *NUMBER***] | mac [***NAME* **|** *NUMBER***] | ipv6 [***NAME* **|** *NUMBER***] | arp [***NAME***]]**

Параметры

ip	(Опционально.) Укажите для отображения всех списков доступа IP.
mac	(Опционально.) Укажите для отображения всех списков доступа MAC.
ipv6	(Опционально.) Укажите для отображения всех списков доступа IPv6.
arp	(Опционально.) Укажите для отображения всех списков доступа ARP.
NAME	(Опционально.) Укажите имя списка доступа для отображения.
NUMBER	(Опционально.) Укажите ID списка доступа для отображения.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения информации о списках доступа. Если не указан определенный параметр, отображается перечень всех настроенных списков доступа. Если указан тип списка доступа, будет отображена подробная информация о соответствующем ему списке доступа. Если включен аппаратный счетчик ACL (ACL hardware counter) для списка доступа (access list), счетчик будет отображен на основе каждой записи списка доступа.

Пример

В данном примере показано, как отобразить все списки доступа.

```
Switch# show access-list

Access-List-Name                                Type
----------------------------------------   ---------------
Strict-Control(ID: 3999)                   ip ext-acl
daily-profile(ID: 7999)                    mac ext-acl
ip6-control(ID: 14999)                     ipv6 ext-acl

Total Entries: 3


Switch#
```

В примере ниже показано, как отобразить списки доступа IP с именем Strict-Control.

```
Switch#show access-list ip Strict-Control

Extended IP access list Strict-Control(ID: 3999)
    10 permit any 10.20.0.0 0.0.255.255
    20 permit any host 10.100.1.2

Switch#
```

В следующем примере показано, как отобразить содержимое списка доступа с включенным аппаратным счетчиком.

```
Switch# show access-list ip simple-ip-acl

Extended IP access simple-ip-acl(ID:3994)
    10 permit tcp any 10.20.0.0 0.0.255.255  (Ing: 6410 packets  Egr: 5201 packets)
    20 permit tcp any host 10.100.1.2   (Ing: 3232 packets  Egr: 0 packets)
    30 permit icmp any any   (Ing: 8758 packets  Egr: 4214 packets)

    Counter enable on following port(s):
 Ingress port(s): eth1/0/5-1/0/8
 Egress port(s): eth1/0/3

Switch#
```

5. Команды управления доступом

5.1 access-class

Данная команда используется для указания списка, которому необходимо ограничить доступ к сессии. Чтобы отменить проверку указанного списка доступа, воспользуйтесь формой **no** этой команды.

access-class *IP-ACL*
no access-class *IP-ACL*

Параметры

IP-ACL	Укажите стандартный список доступа IP-адресов. Поле адреса источника с записью permit или deny определяет, является ли узел доверенным или нет.

По умолчанию

Нет.

Режим ввода команды

Line Configuration Mode.

Использование команды

Данная команда применяется для указания списка, которому необходимо ограничить доступ к сессии. Максимальное число списков доступа – 2. Если два списка доступа уже применены, попытка применить новый список доступа будет отклоняться до тех пор, пока один из примененных списков не будет удален с помощью формы **no** данной команды.

Пример

В данном примере показано, как создать стандартный список доступа IP-адресов и задать его для ограничения доступа через Telnet. Доступ к серверу разрешен только узлу 226.1.1.1.

```
Switch#configure terminal
Switch(config)#ip access-list vty-filter
Switch(config-ip-acl)#permit 226.1.1.1 0.0.0.0
Switch(config-ip-acl)#exit
Switch(config)#line telnet
Switch(config-line)#access-class vty-filter
Switch(config-line)#
```

5.2 do

Данная команда используется для выполнения команд, изначально находящихся в режиме EXEC Mode, из режима глобальной конфигурации.

do *COMMAND*

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда применяется для выполнения команд, изначально находящихся в режиме EXEC Mode (таких как **show**, **clear** или **debug**) при настройке коммутатора. После выполнения команды произойдет возврат системы к используемому режиму конфигурации.

Примечание: в команде можно использовать знак вопроса (?) и клавишу Tab.

Пример

В данном примере показано, как использовать в команде знак вопроса (?).

```
Switch# configure terminal
Switch(config)#do show running-config ?
  all         All configurations including commands corresponding to default
              parameters
  effective   The configurations which affect the behavior of the device
  interface   Select an interface
  Vlan        VLAN configuration
  |           Output modifiers
  <cr>

Switch(config)#do show running-config
```

В данном примере показано, как выполнить команду **show ip interface** в режиме Global Configuration Mode.

```
Switch#configure terminal
Switch(config)#do show ip interface

Interface vlan1 is enabled, Link status is down
  IP Address is 10.90.90.90/8 (Manual)
  ARP timeout is 240 minutes.

Total Entries: 1

Switch(config)#
```

5.3 ip http server

Данная команда используется для включения сервера HTTP. Чтобы отключить сервер HTTP, воспользуйтесь формой **no** этой команды.

ip http server

no ip http server

Параметры

Нет.

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда применяется для включения или отключения сервера HTTP. Управление интерфейсом доступа HTTPS выполняется отдельно с помощью команд SSL.

Пример

В данном примере показано, как включить сервер HTTP.

```
Switch#configure terminal
Switch(config)#ip http server
Switch(config)#
```

5.4 ip http secure-server

Данная команда используется для включения сервера HTTPS. При использовании команды **ip http secure-server ssl-service-policy** необходимо указать политику сервиса SSL для HTTPS. Чтобы отключить сервер HTTPS, воспользуйтесь формой **no** этой команды.

ip http secure-server [ssl-service-policy *POLICY-NAME***]**

no ip http secure-server

Параметры

ssl-service-policy *NAME*	*POLICY-*	(Опционально.) Укажите имя политики сервиса SSL. Используйте параметр **ssl-service-policy**, только если политика сервиса SSL уже указана с помощью команды **ssl-service-policy**.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда позволяет включить сервер HTTPS и использовать определенную политику сервиса SSL для HTTPS. Если данный параметр не указан, для HTTPS будет использоваться встроенный локальный сертификат.

Пример

В данном примере показано, как включить HTTPS-сервер и использовать политику «sp1» для HTTPS.

```
Switch#configure terminal
Switch(config)#ip http secure-server ssl-service-policy sp1
Switch(config)#
```

5.5 ip {http | https} access-class

Данная команда позволяет назначить список, которому необходимо ограничить доступ к HTTP- или HTTPs-серверу. Для отмены проверки указанного списка доступа воспользуйтесь формой **no** этой команды.

ip {http | https} access-class *IP-ACL*

no ip {http | https} access-class *IP-ACL*

Параметры

IP-ACL	Укажите стандартный список доступа IP-адресов. Поле адреса источника в правиле определяет, является ли узел доверенным.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда позволяет указать список, которому необходимо ограничить доступ к HTTP- или HTTPS-серверу. Если указанный список доступа не существует, команда не будет выполнена и ни один из списков доступа не будет проверяться при доступе к HTTP или HTTPS.

Пример

В данном примере показано, как создать стандартный список доступа IP и назначить его для доступа к HTTP-серверу. Доступ к серверу разрешен только узлу 226.1.1.1.

```
Switch#configure terminal
Switch(config)#ip access-list http-filter
Switch(config-ip-acl)#permit 226.1.1.1 255.255.255.255
Switch(config-ip-acl)#exit
Switch(config)#ip http access-class http-filter
Switch(config)#
```

5.6 ip http service-port

Данная команда позволяет указать порт для HTTP-соединения. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip http service-port *TCP-PORT*
no ip http service-port

Параметры

TCP-PORT	Укажите номер порта TCP в диапазоне от 1 до 65535. Как правило, для протокола HTTP назначается TCP-порт 80.

По умолчанию

По умолчанию используется порт 80.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда позволяет задать номер TCP-порта для сервера HTTP.

Пример

В данном примере показано, как задать TCP-порт с номером 8080.

```
Switch#configure terminal
Switch(config)#ip http service-port 8080
Switch(config)#
```

5.7 ip http timeout-policy idle

Данная команда позволяет задать значение тайм-аута для подключения к серверу HTTP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip http timeout-policy idle *INT*
no ip http timeout-policy idle

Параметры

INT	Укажите значение таймера. Диапазон значений: от 60 до 36000 секунд.

По умолчанию

По умолчанию значение составляет 180 секунд.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы задать значение тайм-аута для подключения к серверу HTTP.

Пример

В данном примере показано, как настроить тайм-аут. Заданное значение – 100 секунд.

```
Switch#configure terminal
Switch(config)#ip http timeout-policy idle 100
Switch(config)#
```

5.8 ip telnet server

Данная команда используется для включения сервера Telnet. Чтобы отключить сервер Telnet, воспользуйтесь формой **no** этой команды.

ip telnet server
no ip telnet server

Параметры

Нет.

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для включения или отключения сервера Telnet. Интерфейс доступа SSH отдельно управляется командами SSH.

Пример

В данном примере показано, как включить сервер Telnet.

```
Switch#configure terminal
Switch(config)#ip telnet server
Switch(config)#
```

5.9 ip telnet service-port

Данная команда используется, чтобы задать порт, используемый Telnet-сервером. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip telnet service-port *TCP-PORT*
no ip telnet service-port

Параметры

TCP-PORT	Укажите номер TCP-порта. Диапазон значений: от 1 до 65535. Как правило, для Telnet назначается TCP-порт 23.

По умолчанию

По умолчанию используется порт 23.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы указать TCP-порт для доступа по Telnet.

Пример

В данном примере показано, как настроить сервисный порт 3000 для Telnet.

```
Switch#configure terminal
Switch(config)#ip telnet service-port 3000
Switch(config)#
```

5.10 line

Данная команда используется, чтобы задать тип сессии для конфигурации и войти в режим Line Configuration Mode.

line {console | telnet | ssh}

Параметры

console	Укажите локальную консольную сессию терминала.
telnet	Укажите сессию терминала Telnet.
ssh	Укажите сессию терминала SSH.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда позволяет войти в режим Line Configuration Mode.

Пример

В данном примере показано, как войти в режим Line Configuration Mode для сессии терминала SSH и настроить класс доступа «vty-filter».

```
Switch#configure terminal
Switch(config)#line ssh
Switch(config-line)#access-class vty-filter
Switch(config-line)#
```

5.11 show terminal

Данная команда используется, чтобы отобразить информацию о настройках параметров конфигурации терминала для текущей сессии терминала.

show terminal

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить информацию о настройках терминала для текущей сессии.

Пример

В данном примере показано, как отобразить информацию о настройках терминала для текущей сессии.

```
Switch#show terminal
Terminal Settings:
 Length: 24 lines
 Width: 80 columns
 Default Length: 24 lines
 Default Width: 80 columns
 Baud Rate: 115200 bps

Switch#
```

5.12 show ip telnet server

Данная команда используется для отображения информации о состоянии сервера Telnet.

show ip telnet server

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для отображения информации о состоянии сервера Telnet.

Пример

В данном примере показано, как отобразить информацию о состоянии сервера Telnet.

```
Switch#show ip telnet server

Server State: Enabled

Switch#
```

5.13 show ip http server

Данная команда используется для отображения информации о состоянии HTTP-сервера.

show ip http server

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения информации о состоянии HTTP-сервера.

Пример

В данном примере показано, как отобразить информацию о состоянии HTTP-сервера.

```
Switch#show ip http server

ip http server state :  Enabled
Switch#
```

5.14 show ip http secure-server

Данная команда используется для отображения информации о состоянии SSL.

show ip http secure-server

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для отображения информации о состоянии SSL.

Пример

В данном примере показано, как отобразить информацию о состоянии SSL.

```
Switch#show ip http secure-server

ip http secure-server state :  Disabled
Switch#
```

5.15 show users

Данная команда используется для отображения информации об активных сессиях на коммутаторе.

show users

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения информации об активных сессиях на коммутаторе.

Пример

В данном примере показано, как отобразить информацию обо всех сессиях.

```
Switch#show users
ID   Type      User-Name       Login-Time          IP address
-----------------------------------------------------------------------
0    * console admin           25M58S

Total Entries: 1

Switch#
```

5.16 terminal length

Данная команда используется для настройки количества строк, отображаемых на экране. Команда **terminal length** влияет только на текущую сессию. Команда **terminal length default** установит значение по умолчанию, но не повлияет на текущую сессию. Созданный заново терминал будет использовать значение по умолчанию. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

terminal length *NUMBER*
no terminal length
terminal length default *NUMBER*
no terminal length default

Параметры

NUMBER	Укажите количество строк, отображаемых на экране. Диапазон значений: от 0 до 512. При значении 0 отображение не прекратится, пока не будет достигнут конец отображаемого материала.

По умолчанию

Значение по умолчанию – 24.

Режим ввода команды

EXEC Mode для команды **terminal length**.

Global Configuration Mode для команды **terminal length default**.

Использование команды

При значении 0 вывод команд не будет приостанавливаться, пока не будет достигнут конец отображаемого материала.

Если в команде **terminal length** указано значение, отличное от 0 (например, 50), то вывод приостанавливается после каждых 50 строк. Используйте данную команду, чтобы настроить количество отображаемых строк во время текущей сессии. Команда также применяется для сессий Telnet и SSH.

Если вывод одной команды выходит за границы экрана, то такой вывод приостанавливается и в нижней части экрана появляется приглашение **--More--**. При появлении приглашения **--More--** нажмите CTRL+C, q, Q или ESC, чтобы прервать вывод и вернуться к приглашению. Нажмите пробел для отображения дополнительного экрана вывода или нажмите Return для отображения еще одной строки вывода. При настройке длины экрана на 0 отключается функция прокручивания, из-за чего весь вывод

экрана отображается сразу. Пока не будет использовано ключевое слово **default**, изменения значения terminal length будут применяться только к текущей сессии. При использовании формы **no** данной команды количество строк на экране терминала сбрасывается к 24.

Команда **terminal length default** доступна в режиме глобальной конфигурации (Global Configuration Mode). Параметры команды не влияют на текущие сессии терминала, но будут влиять на сессии, активированные позднее. Сохранить можно только значение длины терминала по умолчанию.

Пример

В данном примере показано, как изменить количество строк. Указанное значение – 60.

```
Switch#terminal length 60
Switch#
```

5.17 terminal speed

Данная команда используется для настройки скорости терминала. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

terminal speed *BPS*
no terminal speed

Параметры

BPS	Укажите скорость консоли в бит/с.

По умолчанию

Значение по умолчанию – 115200.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда применяется для настройки скорости подключения терминала. Некоторые скорости передачи данных, доступные на подключенных устройствах, не поддерживаются коммутатором.

Пример

В данном примере показано, как изменить скорость последовательного порта, указав значение 9600 бит/с.

```
Switch#configure terminal
Switch(config)#terminal speed 9600
Switch(config)#
```

5.18 session-timeout

Данная команда используется, чтобы задать значение тайм-аута сессии. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

session-timeout *MINUTES*
no session-timeout

Параметры

MINUTES	Укажите тайм-аут в минутах. При использовании значения 0 тайм-аут не истекает никогда.

По умолчанию

Значение по умолчанию – 3 минуты.

Режим ввода команды

Line Configuration Mode.

Использование команды

Используйте данную команду, чтобы задать значение тайм-аута сессии, по истечении которого произойдет автоматический выход из учетной записи.

Пример

В данном примере задается значение, при котором тайм-аут не истекает никогда.

```
Switch#configure terminal
Switch(config)#line console
Switch(config-line)#session-timeout 0
Switch(config-line)#
```

5.19 terminal width

Данная команда используется для настройки количества столбцов символов, отображаемых на экране для текущей сессии. Команда **terminal width** влияет только на текущую сессию. Команда **terminal width default** установит значение по умолчанию, но не повлияет на текущую сессию. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

terminal width *NUMBER*
no terminal width
terminal width default *NUMBER*
no terminal width default

Параметры

NUMBER	Укажите количество символов, отображаемых на экране. Диапазон значений: от 40 до 255.

По умолчанию

Значение по умолчанию – 80.

Режим ввода команды

EXEC Mode для команды **terminal width**.

Global Configuration Mode для команды **terminal width default**.

Использование команды

Команда **terminal width** позволяет изменить ширину терминала и применяется только к текущей сессии. При использовании формы **no** команда вернет значение по умолчанию.

Команда **terminal width default** доступна в режиме глобальной конфигурации (Global Configuration Mode). Параметры команды не влияют на текущие сессии терминала, но будут влиять на сессии, активированные позднее. Сохранить можно только значение ширины терминала по умолчанию.

Однако при удаленном доступе к сессии CLI, например, Telnet, ширина терминала автосогласования будет иметь преимущество над настройками по умолчанию, если согласование прошло успешно. В противном случае будут применяться настройки по умолчанию.

Пример

В данном примере показано, как изменить текущую ширину терминала, указав значение 120.

```
Switch#terminal width 120
Switch#
```

5.20 username

Данная команда используется для создания учетной записи пользователя. Чтобы удалить учетную запись пользователя, воспользуйтесь формой **no** этой команды.

username *NAME* **[nopassword | password** *PASSWORD***]**

no username [*NAME***]**

Параметры

NAME	Укажите имя пользователя. Максимальное количество символов – 32.
nopassword	(Опционально.) Укажите, чтобы для данной учетной записи не применялся пароль.
password	(Опционально.) Укажите, чтобы для данной учетной записи применялся пароль.
PASSWORD	(Опционально.) Укажите пароль на основе одного из указанных выше параметров.

По умолчанию

По умолчанию имя пользователя – *admin*, пароль – *admin*.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда применяется для создания учетной записи пользователя. При входе в систему будет включен режим EXEC Mode.

При использовании команды **no username** без указания имени пользователя удалятся все пользователи.

Если учетная запись пустая, пользователю будет сразу назначен режим EXEC Mode.

Пример

В данном примере показано, как создать учетную запись администратора с именем «admin» и паролем «mypassword».

```
Switch# configure terminal
Switch(config)# username admin password mypassword
Switch(config)#
```

В данном примере показано, как удалить учетную запись с именем «admin».

```
Switch# configure terminal
Switch(config)# no username admin
Switch(config)#
```

5.21 clear line

Данная команда используется для завершения сессии подключения.

clear line *LINE-ID*

Параметры

LINE-ID	Укажите идентификатор line ID сессии соединения, которую необходимо отключить.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Использование команды

Данная команда применяется для отключения активной сессии коммутатора. Идентификатор (line ID) присваивается при создании сессии подключения. Используйте команду **show users** для просмотра активных сессий.

Данная команда может отключить только сессии SSH и Telnet.

Пример

В данном примере показано, как отключить сессию 1.

```
Switch#clear line 1
Switch#
```

6. Команды предотвращения атак ARP Spoofing

6.1 ip arp spoofing-prevention

Данная команда используется для настройки записи ARP Spoofing Prevention (ASP), используемой для предотвращения атак ARP Spoofing. Для удаления записи ARP Spoofing Prevention воспользуйтесь формой **no** этой команды.

ip arp spoofing-prevention *GATEWAY-IP GATEWAY-MAC* **interface** *INTERFACE-ID* **[,|-]**
no ip arp spoofing-prevention *GATEWAY-IP* **[interface** *INTERFACE-ID* **[,|-]]**

Параметры

GATEWAY-IP	Укажите IP-адрес шлюза.
GATEWAY-MAC	Укажите MAC-адрес шлюза. Настройки MAC-адреса заменят последнюю конфигурацию для того же IP-адреса шлюза.
interface *INTERFACE-ID*	Укажите интерфейс, который будет активирован или удален из числа активных интерфейсов (при использовании формы **no**). Запись ARP не будет проверяться, если принимающий порт не включен в указанный список интерфейсов.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию записей нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и port-channel.

Команда используется для создания записи ARP Spoofing Prevention (ASP), чтобы предотвратить спуфинг MAC-адреса защищенного шлюза. После создания записи ARP-пакеты, у которых IP-адрес источника совпадает с IP-адресом шлюза, а MAC-адрес источника не совпадает с MAC-адресом шлюза, будут отбрасываться. ASP игнорирует ARP-пакеты, если IP-адрес источника не совпадает с настроенным IP-адресом шлюза.

Если адрес ARP совпадает с настроенным IP-адресом шлюза, MAC-адресом и списком портов, то проверка Dynamic ARP Inspection (DAI) будет игнорироваться независимо от того, является ли порт ARP доверенным или нет.

Пример

В данном примере показано, как настроить запись ARP Spoofing Prevention с IP-адресом 10.254.254.251 и MAC-адресом 00-00-00-11-11-11 для Ethernet-порта 1/0/10.

```
Switch# configure terminal
Switch(config)# ip arp spoofing-prevention 10.254.254.251 00-00-00-11-11-11 interface
eth1/0/10
Switch(config)# ip arp spoofing-prevention 10.254.254.251 00-00-00-11-11-11 interface port-
channel 3
Switch(config)#
```

6.2 show ip arp spoofing-prevention

Данная команда используется для отображения настроек ARP Spoofing Prevention.

show ip arp spoofing-prevention

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения всех записей ARP Spoofing Prevention.

Пример

В данном примере показано, как отобразить записи ARP Spoofing Prevention.

```
Switch#show ip arp spoofing-prevention

IP              MAC               Interfaces
--------------- ----------------- ----------------------------
10.254.254.251  00-00-00-11-11-11 eth1/0/10

Total Entries: 1

Switch#
```

Отображаемые параметры

IP	IP-адрес шлюза.
MAC	MAC-адрес шлюза.
Interfaces	Интерфейсы, на которых активна функция предотвращения атак ARP Spoofing.

7. Команды Asymmetric VLAN

7.1 asymmetric-vlan

Данная команда используется для включения функции Asymmetric VLAN. Для отключения функции воспользуйтесь формой **no** этой команды.

asymmetric-vlan
no asymmetric-vlan

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда применяется для включения/отключения функции Asymmetric VLAN.

Пример

В данном примере показано, как запустить функцию Asymmetric VLAN.

```
Switch# configure terminal
Switch(config)# asymmetric-vlan
```

В данном примере показано, как отключить функцию Asymmetric VLAN.

```
Switch# configure terminal
Switch(config)# no asymmetric-vlan
```

8. Команды Authentication, Authorization и Accounting (AAA)

8.1 aaa authentication dot1x

Данная команда позволяет настроить список методов по умолчанию, используемый для аутентификации 802.1X. Для удаления списка методов по умолчанию воспользуйтесь формой **no** этой команды.

aaa authentication dot1x default *METHOD1* **[***METHOD2***...]**
no aaa authentication dot1x default

Параметры

METHOD1 **[***METHOD2***...]**	Укажите список методов, который необходимо выполнить алгоритму аутентификации в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для указания метода. • **local** – для аутентификации используется локальная база данных. • **group radius** – используются серверы, определенные командой RADIUS server host. • **group** *GROUP-NAME* – используются группы серверов, определенные командой AAA group server. • **none** – как правило, данный метод указывается в списке последним. Пользователь пройдет аутентификацию, если это не запрещено предыдущим методом аутентификации.

По умолчанию

Метод аутентификации AAA не настроен.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить список методов по умолчанию для аутентификации 802.1X. Аутентификация запросов 802.1X будет выполняться на основе локальной базы данных.

Пример

В данном примере показано, как установить список методов по умолчанию для аутентификации пользователей dot1X.

```
Switch#configure terminal
Switch(config)#aaa authentication dot1x default group radius
Switch(config)#
```

8.2 aaa group server radius

Данная команда используется для входа в режим настройки группы серверов RADIUS и привязки серверов к группе. Для удаления группы серверов RADIUS воспользуйтесь формой **no** этой команды.

aaa group server radius *GROUP-NAME*
no aaa group server radius *GROUP-NAME*

Параметры

GROUP-NAME	Укажите название группы серверов. Максимальное количество символов – 32. Синтаксисом является обычная строка, пробелы недопустимы.

По умолчанию

Группа серверов AAA не настроена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда позволяет определить группу серверов RADIUS. Созданная группа серверов используется для установки списков методов, используемых для аутентификации или аккаунтинга с помощью команды **aaa authentication**. Также команда применяется, чтобы войти в режим настройки группы серверов RADIUS (RADIUS Group Server Configuration Mode). Используйте команду **server** для привязки серверов RADIUS к группе.

Пример
В данном примере показано, как создать группу серверов RADIUS с двумя записями. Второй узел выступает в качестве резервного сервера.

```
Switch# configure terminal
Switch(config)#aaa group server radius group1
Switch(config-sg-radius)# server 172.19.10.100
Switch(config-sg-radius)# server 172.19.11.20
Switch(config-sg-radius)# exit
Switch(config)#
```

8.3 aaa new-model

Данная команда используется, чтобы включить функцию AAA для аутентификации. Для отключения данной функции воспользуйтесь формой **no** этой команды.

aaa new-model
no aaa new-model

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду для включения функции AAA. Данная функция должна быть включена до того, как начнет действовать аутентификация по спискам методов AAA. Если функция AAA отключена, пользователь будет аутентифицирован через локальную таблицу учетных записей, созданную командой **username**.

Пример

В данном примере показано, как включить функцию AAA.

```
Switch#configure terminal
Switch(config)#aaa new-model
Switch(config)#
```

8.4 clear aaa counters servers

Данная команда используется для сброса счетчиков статистики серверов AAA.

clear aaa counters servers {all | radius {*IP-ADDRESS* **|** *IPV6-ADDRESS* **| all} | sg** *NAME***}**

Параметры

all	Укажите, чтобы сбросить счетчики для всех серверов.
radius *IP-ADDRESS*	Укажите, чтобы сбросить счетчики для заданного сервера RADIUS IPv4.
radius *IPV6-ADDRESS*	Укажите, чтобы сбросить счетчики для заданного сервера RADIUS IPv6.
radius all	Укажите, чтобы сбросить счетчики для всех серверов RADIUS.
sg *NAME*	Укажите, чтобы сбросить счетчики для всех серверов в указанной группе.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду для сброса счетчиков статистики, относящихся к серверам AAA.

Пример

В данном примере показано, как сбросить счетчики серверов AAA.

```
Switch#clear aaa counters servers all
Switch#
```

В примере ниже показано, как удалить информацию счетчиков серверов AAA для всех узлов в группе серверов «server-farm».

```
Switch#clear aaa counters servers sg server-farm
Switch#
```

8.5 radius-server deadtime

Данная команда используется для назначения интервала времени, в течение которого разрешается пропускать опрос недоступного сервера. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

radius-server deadtime *MINUTES*
no radius-server deadtime

Параметры

MINUTES	Укажите время простоя. Диапазон значений: от 0 до 1440 (24 часа). Если установлено значение 0, недоступный сервер не будет помечен как недействующий.

По умолчанию

По умолчанию используется значение 0.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда позволяет оптимизировать время обработки данных аутентификации с помощью установки времени простоя (dead time), в течение которого недоступные серверы опрашиваться не будут.

Система, выполняющая аутентификацию с помощью сервера аутентификации, пробует использовать каждый сервер поочередно. Если сервер не отвечает, система будет пробовать следующий сервер. Система отметит сервер, который не отвечает, как недействующий, запустит таймер времени простоя и пропустит такой сервер при аутентификации последующих запросов до истечения заданного времени простоя.

Пример

В данном примере показано, как установить время простоя. Настроенное значение – 10 минут.

```
Switch#configure terminal
Switch(config)#radius-server deadtime 10
Switch(config)#
```

8.6 radius-server host

Данная команда используется для добавления RADIUS-сервера в список используемых серверов. Чтобы удалить сервер, воспользуйтесь формой **no** этой команды.

radius-server host {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [auth-port** *PORT***] [timeout** *SECONDS***] [retransmit** *COUNT***] key** *KEY-STRING*

no radius-server host {*IP-ADDRESS* **|** *IPV6-ADDRESS***}**

Параметры

IP-ADDRESS	Укажите IP-адрес RADIUS-сервера.
IPV6-ADDRESS	Укажите IPv6-адрес RADIUS-сервера.
auth-port *PORT*	(Опционально.) Укажите номер UDP-порта назначения для отправки пакетов аутентификации. Диапазон значений: от 0 до 65535. Установите ноль в качестве значения номера порта, если сервер не предназначен для аутентификации. Значение по умолчанию – 1812.
timeout *SECONDS*	(Опционально.) Укажите значение тайм-аута сервера. Диапазон значений: от 1 до 255 секунд. Если значение не указано, по умолчанию используется 5 секунд.
retransmit *COUNT*	(Опционально.) Укажите количество повторных передач запросов на сервер, когда ответ не получен. Диапазон значений: от 0 до 20. Используйте 0 для отключения повторной передачи. Если значение не указано, по умолчанию используется 2.
key *KEY-STRING*	Укажите ключ, используемый для связи с сервером. Ключ может содержать от 1 до 254 символов незашифрованного текста.

По умолчанию

По умолчанию сервер не настроен.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду для создания RADIUS-серверов перед тем, как они могут быть связаны с группой серверов RADIUS с помощью команды **server**.

Пример

В данном примере показано, как создать два RADIUS-сервера с разными IP-адресами.

```
Switch# configure terminal
Switch(config)# radius-server host 172.19.10.100 auth-port 1500 timeout 8 retransmit 3 key
ABCDE
Switch(config)# radius-server host 172.19.10.101 auth-port 1600 timeout 3 retransmit 1 key
ABCDE
Switch(config)#
```

8.7 server (RADIUS)

Данная команда используется для привязки RADIUS-сервера к группе RADIUS-серверов. Для удаления сервера из группы воспользуйтесь формой **no** этой команды.

server {*IP-ADDRESS* **|** *IPV6-ADDRESS***}**
no server {*IP-ADDRESS* **|** *IPV6-ADDRESS***}**

Параметры

IP-ADDRESS	Укажите IPv4-адрес сервера аутентификации.
IPV6-ADDRESS	Укажите IPv6-адрес сервера аутентификации.

По умолчанию

По умолчанию сервер не настроен.

Режим ввода команды

RADIUS Group Server Configuration Mode.

Использование команды

Команда **server** применяется для привязки RADIUS-сервера к группе серверов RADIUS. Определенная группа серверов может быть указана в качестве списка методов аутентификации или аккаунтинга с помощью команды **aaa authentication**. Команда **radius-server host** позволяет создать запись сервера. Данная запись идентифицируется по IP-адресу.

Пример

В данном примере показано, как задать два RADIUS-сервера с разными IP-адресами, а затем создать группу серверов с использованием данных RADIUS-серверов.

```
Switch#configure terminal
Switch(config)#radius-server host 172.19.10.100 auth-port 1500 timeout 8 retransmit 3 key
ABCDE
Switch(config)#radius-server host 172.19.10.101 auth-port 1600 timeout 3 retransmit 1 key
ABCDE
Switch(config)#aaa group server radius group1
Switch(config-sg-radius)#server 172.19.10.100
Switch(config-sg-radius)#server 172.19.10.101
Switch(config-sg-radius)#
```

8.8 show aaa

Данная команда используется для отображения глобального состояния AAA.

show aaa

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду для отображения глобального состояния AAA.

Пример

В данном примере показано, как отобразить глобальное состояние AAA.

```
Switch#show aaa

AAA is enabled.

Switch#
```

8.9 show radius statistics

Данная команда используется, чтобы отобразить статистику RADIUS для пакетов аутентификации.

show radius statistics

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду для отображения счетчиков статистики, относящихся к серверам.

Пример

В данном примере показано, как отобразить счетчики статистики, относящиеся к серверам.

```
Switch#show radius statistics

 RADIUS Server: 172.19.10.100: Auth-Port 1500
 State is Up
                        Auth.
 Round Trip Time:       0
 Access Requests:       0
 Access Accepts:        0
 Access Rejects:        0
 Access Challenges:     0
 Retransmissions:       0
 Malformed Responses:   0
 Bad Authenticators:    0
 Pending Requests:      0
 Timeouts:              0
 Unknown Types:         0
 Packets Dropped:       0

 RADIUS Server: 172.19.10.101: Auth-Port 1600
 State is Up
                        Auth.
 Round Trip Time:       0
 Access Requests:       0
 Access Accepts:        0
 Access Rejects:        0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Отображаемые параметры

Auth.	Статистика для пакетов аутентификации.
Round Trip Time	Интервал времени (в сотых долях секунды) между последним ответом и запросом, который соответствует ему, с этого сервера RADIUS.
Access Requests	Количество пакетов RADIUS Access-Request, отправленных на данный сервер. Не включает повторные передачи.
Access Accepts	Количество пакетов RADIUS Access-Accept (действительных или недействительных), полученных с данного сервера.
Access Rejects	Количество пакетов RADIUS Access-Reject (действительных или недействительных), полученных с данного сервера.
Access Challenges	Количество пакетов RADIUS Access-Challenge (действительных или недействительных), полученных с данного сервера.
Retransmissions	Количество пакетов RADIUS Request, повторно переданных данному RADIUS-серверу. Повторные передачи включают попытки, при которых поля Identifier и Acct-Delay были обновлены, а также попытки, при которых они остаются без изменений.

Malformed Responses	Количество ошибочных пакетов RADIUS Response, полученных от данного сервера. Ошибочные пакеты включают пакеты с некорректной длиной. Неверные аутентификаторы, атрибуты Signature или неизвестные типы не учитываются.
Bad Authenticators	Количество пакетов RADIUS Response, полученных от данного сервера и содержащих некорректные аутентификаторы или атрибуты Signature.
Pending Requests	Количество пакетов RADIUS Request, предназначенных для данного сервера, время которых еще не истекло, или которые не получили ответ. Эта переменная увеличивается, когда запрос отправляется, и уменьшается из-за получения ответа, тайм-аута или повторной передачи.
Timeouts	Количество тайм-аутов для данного сервера. По истечении тайм-аута клиент может повторить попытку подключения к данному серверу, отправить запрос на аутентификацию другому серверу или прекратить попытки. Повторная попытка подключиться к этому же серверу считается повторной передачей, также как и тайм-аут. Попытка подключиться к другому серверу рассматривается как запрос, точно также как и тайм-аут.
Unknown Types	Количество пакетов RADIUS неизвестного типа, полученных от данного сервера.
Packets Dropped	Количество пакетов RADIUS, полученных от данного сервера и отброшенных по какой-либо причине.

9. Базовые команды настройки IPv4

9.1 arp

Данная команда используется для добавления статической записи в кэш ARP (Address Resolution Protocol). Для удаления статической записи из кэша ARP воспользуйтесь формой **no** этой команды.

arp *IP-ADDRESS HARDWARE-ADDRESS*
no arp *IP-ADDRESS HARDWARE-ADDRESS*

Параметры

IP-ADDRESS	Укажите IP-адрес.
HARDWARE-ADDRESS	Укажите MAC-адрес (48-битный).

По умолчанию

В кэше ARP нет ни одной статической записи.

Режим ввода команды

Global Configuration Mode.

Использование команды

Таблица ARP обеспечивает сопоставление IP-адресов с MAC-адресами. Данное соответствие хранится в памяти и не запрашивается постоянно. Указанная команда используется для добавления статических ARP-записей.

Пример

В данном примере показано, как добавить статическую ARP-запись для Ethernet-узла.

```
Switch# configure terminal
Switch(config)# arp 10.31.7.19 0800.0900.1834
Switch(config)#
```

9.2 arp timeout

Данная команда используется для настройки времени устаревания (aging time) ARP-записей в таблице ARP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

arp timeout *MINUTES*
no arp timeout

Параметры

MINUTES	Укажите таймаут, по истечении которого динамическая запись устареет при условии отсутствия сетевой активности. Диапазон значений: от 0 до 65535 минут. Если указать 0, то записи ARP никогда не будут устаревать.

По умолчанию

Значение по умолчанию – 240 минут.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда используется для настройки времени устаревания ARP-записей в таблице ARP.

Пример

В данном примере показано, как задать тайм-аут продолжительностью 60 минут.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# arp timeout 60
Switch(config-if)#
```

9.3 clear arp-cache

Данная команда используется для удаления динамических ARP-записей из таблицы.

clear arp-cache {all | interface *INTERFACE-ID* **|** *IP-ADDRESS***}**

Параметры

all	Укажите, чтобы полностью очистить кэш динамических ARP-записей, связанных со всеми интерфейсами.
interface *INTERFACE-ID*	Укажите идентификатор интерфейса.
IP-ADDRESS	Укажите IP-адрес динамической ARP-записи, которую необходимо удалить.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для удаления динамических записей из таблицы ARP. Пользователь может удалить сразу все динамические записи, только выбранные динамические записи или все динамические записи для конкретного интерфейса.

Пример

В данном примере показано, как удалить все динамические записи из кэша ARP.

```
Switch# clear arp-cache all
Switch#
```

9.4 ip address

Данная команда используется для назначения интерфейсу основного или второстепенного адреса IPv4, а также для автоматического получения IP-адреса от DHCP-сервера. Чтобы удалить настройки IP-адреса или отключить DHCP на интерфейсе, воспользуйтесь формой **no** этой команды.

ip address {*IP-ADDRESS SUBNET-MASK* **| dhcp}**
no ip address [*IP-ADDRESS SUBNET-MASK* **| dhcp]**

Параметры

IP-ADDRESS	Укажите IP-адрес.
SUBNET-MASK	Укажите маску подсети для соответствующего IP-адреса.
dhcp	Укажите, чтобы получить IP-адрес от DHCP-сервера.

По умолчанию

IP-адрес по умолчанию для VLAN 1 – 10.90.90.90/8.

Режим ввода команды

Interface Configuration Mode.

Использование команды

IPv4-адрес интерфейса может быть задан пользователем вручную или динамически (автоматически) назначен сервером DHCP. Для удаления заданного IP-адреса воспользуйтесь командой **no ip address**.

Примечание: максимальное количество интерфейсов IPv4/IPv6 на коммутаторе – 4.

Пример

В данном примере показано, как настроить 10.108.1.27 в качестве IP-адреса для VLAN 1.

```
Switch# configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip address 10.108.1.27 255.0.0.0
Switch(config-if)#
```

9.5 show arp

Данная команда используется для отображения данных кэша ARP.

show arp [*ARP-TYPE***] [***IP-ADDRESS* **[***MASK***]] [***INTERFACE-ID***] [***HARDWARE-ADDRESS***]**

Параметры

ARP-TYPE	(Опционально.) Укажите тип ARP. **dynamic** – для отображения только динамических ARP-записей. **static** – для отображения только статических ARP-записей.
IP-ADDRESS **[***MASK***]**	(Опционально.) Укажите, если необходимо отобразить определенную запись или записи определенной сети.
INTERFACE-ID	(Опционально.) Укажите, если необходимо отобразить ARP-записи, связанные с определенным интерфейсом.
HARDWARE-ADDRESS	(Опционально.) Укажите, если необходимо отобразить ARP-записи, аппаратный адрес которых равен данному MAC-адресу.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить информацию для определенной ARP-записи, всех ARP-записей, динамических или статических записей, а также для записей, связанных с определенным IP-интерфейсом.

Пример

В данном примере показано, как отобразить данные кэша ARP.

```
Switch# show arp

S - Static Entry

IP Address         Hardware Addr      IP Interface   Age (min)
-----------------  -----------------  -------------  ---------------
S 10.31.7.19       08-00-09-00-18-34  vlan1          forever
  10.90.90.90      00-01-02-03-04-00  vlan1          forever

Total Entries: 2

Switch#
```

9.6 show arp timeout

Данная команда используется для отображения времени устаревания записей в кэше ARP.

show arp timeout [interface *INTERFACE-ID***]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите идентификатор интерфейса.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения заданного времени устаревания ARP-записей.

Пример

В данном примере показано, как отобразить время устаревания ARP-записей.

```
Switch# show arp timeout

Interface    Timeout (minutes)
------------ -----------------
vlan1        60
------------ -----------------
Total Entries:1

Switch#
```

9.7 show ip interface

Данная команда используется для отображения информации по IP-интерфейсам.

show ip interface [*INTERFACE-ID***] [brief]**

Параметры

INTERFACE-ID	(Опционально.) Укажите, чтобы отобразить информацию по определенному IP-интерфейсу.
brief	(Опционально.) Укажите, чтобы отобразить краткую информацию по IP-интерфейсам.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если параметры не указаны, будет отображаться информация для всех интерфейсов.

Пример

В данном примере показано, как отобразить краткую информацию по IP-интерфейсам.

```
Switch#show ip interface brief

Interface    IP Address      Link Status
---------- --------------- -----------
vlan1       10.90.90.90      up

Total Entries: 1

Switch#
```

В примере ниже показано, как отобразить информацию для интерфейса VLAN 1.

```
Switch#show ip interface vlan 1

Interface vlan1 is enabled, Link status is down
  IP address is 10.90.90.90/8 (Manual)
  ARP timeout is 240 minutes.
  gratuitous-send is disabled, interval is 0 seconds

Total Entries: 1

Switch#
```

10. Базовые команды настройки IPv6

10.1 clear ipv6 neighbors

Данная команда используется для удаления динамических записей из IPv6 neighbor cache.

clear ipv6 neighbors {all | interface *INTERFACE-ID***}**

Параметры

all	Укажите, чтобы удалить динамические записи из IPv6 neighbor cache для всех интерфейсов.
interface *INTERFACE-ID*	Укажите, чтобы удалить динамические записи из IPv6 neighbor cache для конкретного интерфейса.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется только для удаления динамических записей из IPv6 neighbor cache.

Пример

В примере показано, как очистить IPv6 neighbor cache для интерфейса VLAN 1.

```
Switch# clear ipv6 neighbors interface vlan 1
Switch#
```

10.2 ipv6 address

Данная команда используется для настройки IPv6-адреса вручную на интерфейсе. Чтобы удалить заданный вручную IPv6-адрес, воспользуйтесь формой **no** этой команды.

ipv6 address {*IPV6-ADDRESS/PREFIX-LENGTH* **|** *IPV6-ADDRESS* **link-local}**

no ipv6 address {*IPV6-ADDRESS/PREFIX-LENGTH* **|** *IPV6-ADDRESS* **link-local}**

Параметры

IPV6-ADDRESS	Укажите IPv6-адрес и длину префикса для подсети.
PREFIX-LENGTH	Укажите длину префикса. Префикс IPv6-адреса также является локальной подсетью на интерфейсе.
link-local	Укажите адрес Link-Local.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

IPv6-адрес может быть задан пользователем вручную или назначен с использованием основного префикса, получаемого клиентом DHCPv6. Если использование команды **ipv6 address** не планируется, то предварительное получение основного префикса не требуется. Для настройки IPv6-адреса основной префикс необходимо получить заранее. Заданный IPv6-адрес будет удален, если тайм-аут получения основного префикса истек или префикс удален. IPv6-адрес формируется с использованием основного префикса в главной части битов, исключая часть основного префикса в оставшейся части битов.

Интерфейсу можно назначить один IPv6-адрес. После завершения настройки IPv6-адреса интерфейс получает разрешение на обработку IPv6. Префикс заданного IPv6-адреса автоматически анонсируется в качестве префикса в передаваемых интерфейсом сообщениях RA.

Пример

В данном примере показано, как задать IPv6-адрес.

```
Switch# configure terminal
Switch(config)# interface vlan 2
Switch(config-if)# ipv6 address 3ffe:22:33:44::55/64
```

В примере ниже показано, как удалить IPv6-адрес.

```
Switch# configure terminal
Switch(config)# interface vlan 2
Switch(config-if)# no ipv6 address 3ffe:22:3:44::55/64
```

10.3 ipv6 address eui-64

Данная команда позволяет настроить на интерфейсе IPv6-адрес с использованием идентификатора интерфейса EUI-64 (Interface ID). Для удаления IPv6-адреса, сгенерированного с использованием идентификатора интерфейса EUI-64, воспользуйтесь формой **no** этой команды.

ipv6 address *IPV6-PREFIX/PREFIX-LENGTH* **eui-64**

no ipv6 address *IPV6-PREFIX/PREFIX-LENGTH* **eui-64**

Параметры

IPV6-PREFIX	Укажите IPv6-префикс для конфигурируемого IPv6-адреса.
PREFIX-LENGTH	Укажите длину префикса. Префикс IPv6-адреса также является локальной подсетью на интерфейсе. Максимальная длина префикса – 64.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Если данная команда сконфигурирована в туннеле ISATAP (IPv6), то последние 32 бита идентификатора интерфейса (Interface ID) формируются с использованием IPv4-адреса источника туннеля.

Пример

В данном примере показано, как добавить IPv6-адрес.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 address 3ffe:501:ffff:0::/64 eui-64
Switch(config-if)#
```

10.4 ipv6 address dhcp

Данная команда используется для настройки интерфейса на получение IPv6-адреса с помощью DHCPv6. Чтобы отключить использование DHCPv6 для получения IPv6-адреса, воспользуйтесь формой **no** этой команды.

ipv6 address dhcp [rapid-commit]

no ipv6 address dhcp

Параметры

rapid-commit	(Опционально.) Укажите, чтобы получить адрес от сервера при помощи обмена двумя сообщениями. Опция rapid-commit будет встроена в сообщение Solicit, чтобы запросить подтверждение при помощи обмена двумя сообщениями.

По умолчанию

Данная опция по умолчанию отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить на интерфейсе получение сетевых настроек IPv6 от DHCPv6-сервера.

Стандартный обмен сообщениями между маршрутизаторами Delegating Router (DR) и Requesting Router (RR) включает в себя четыре сообщения: *SOLICIT, ADVERTISE, REQUEST* и *REPLY*. При использовании параметра **rapid-commit** маршрутизаторы обмениваются двумя сообщениями вместо четырех. В этом случае маршрутизатор RR отправит маршрутизатору DR сообщение SOLICIT, в котором уведомит его о возможности пропустить получение сообщения ADVERTISE и отправку сообщения REQUEST и перейти непосредственно к получению сообщения REPLY от маршрутизатора DR. В сообщении REPLY содержится информация по сетевым настройкам.

Для корректной работы данного функционала необходимо включить параметр **rapid-commit** как на DR, так и на RR.

При использовании данной команды с формой **no** текущие сетевые настройки IPv6, полученные от DHCPv6-сервера, будут удалены.

Пример

В данном примере показано, как настроить получение IPv6-адреса от DHCPv6-сервера на интерфейсе VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 address dhcp
Switch(config-if)#
```

10.5 ipv6 address autoconfig

Данная команда используется для автоматической настройки IPv6-адреса с помощью механизма автоконфигурации Stateless Auto-Configuration. Чтобы удалить IPv6-адрес, сгенерированный с помощью механизма автоконфигурации, воспользуйтесь формой **no** этой команды.

ipv6 address autoconfig [default]
no ipv6 address autoconfig

Параметры

default	(Опционально.) Если на данном интерфейсе выбран шлюз по умолчанию, то с указанием параметра default будет установлен маршрут по умолчанию с использованием этого шлюза по умолчанию. Параметр можно указать только на одном интерфейсе.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда доступна только для интерфейса VLAN IPv6.

При включении автоконфигурации интерфейс включает обработку IPv6 и получает анонс от маршрутизатора IPv6 с назначенным префиксом глобального адреса. Далее итоговый адрес,

состоящий из префикса и идентификатора интерфейса, назначается данному интерфейсу. В случае отключения этой опции полученный Global Unicast-адрес будет удален из интерфейса.

Применение опции **default** позволит использовать анонс маршрутизатора для добавления маршрута по умолчанию в таблицу маршрутизации IPv6. Данный маршрут по умолчанию получен с помощью SLAAC и обладает более высоким приоритетом по сравнению с другими динамическими маршрутами, полученными по протоколам RIPng, OSPFv3 и BGP+, но более низким приоритетом по сравнению со статическими маршрутами по умолчанию.

Пример

В данном примере показано, как автоматически сконфигурировать IPv6-адрес, используя механизм Stateless Auto-Configuration.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 address autoconfig
Switch(config-if)#
```

10.6 ipv6 enable

Данная команда используется для включения обработки IPv6 на интерфейсах, у которых нет явно настроенного IPv6-адреса. Чтобы отключить обработку IPv6 на интерфейсах, у которых нет явно настроенного IPv6-адреса, воспользуйтесь формой **no** этой команды.

ipv6 enable
no ipv6 enable

Параметры

Нет.

По умолчанию

Данная опция по умолчанию отключена.

Режим ввода команды

Interface Configuration Mode

Использование команды

Если IPv6-адрес задан на интерфейсе явно, автоматически генерируется IPv6-адрес Link-Local и начинается обработка IPv6. Если на интерфейсе нет явно настроенного IPv6-адреса, IPv6-адрес Link-Local не генерируется и обработка IPv6 не запускается. Используйте команду **ipv6 enable** для автоматической генерации IPv6-адреса Link-Local и запуска обработки IPv6 на интерфейсе.

Пример

В данном примере показано, как включить поддержку IPv6 на интерфейсе VLAN 1, у которого нет явно настроенного IPv6-адреса.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 enable
Switch(config-if)#
```

10.7 ipv6 hop-limit

Данная команда используется, чтобы настроить параметр hop limit (предельное число шагов) для IPv6 на коммутаторе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 hop-limit *VALUE*
no ipv6 hop-limit

Параметры

VALUE	Укажите значение для параметра IPv6 hop limit. 0 означает, что для отправки пакета используются настройки по умолчанию. Диапазон значений: от 0 до 255.

По умолчанию

Значение по умолчанию – 64.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Используйте данную команду для настройки параметра hop limit, который будет анонсироваться в сообщениях RA. Пакет IPv6, сгенерированный в системе, также будет использовать этот параметр в качестве начального значения hop limit.

Пример

В данном примере показано, как задать значение hop limit для IPv6. Заданное значение – 255.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 hop-limit 255
Switch(config-if)#
```

10.8 ipv6 nd managed-config-flag

Данная команда используется для включения флага Managed Address Configuration (M) в анонсируемых сообщениях RA. Чтобы отключить флаг, воспользуйтесь формой **no** этой команды.

ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag

Параметры

Нет.

По умолчанию

Данный функционал по умолчанию отключен.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Если соседний узел получает сообщение RA с установленным флагом, то для получения IPv6-адресов он должен использовать протокол конфигурации с отслеживанием состояния (Stateful Configuration).

Пример

В данном примере показано, как включить флаг M в сообщениях RA, анонсируемых в VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 nd managed-config-flag
Switch(config-if)#
```

10.9 ipv6 nd other-config-flag

Данная команда используется для включения флага Other Configuration (O) в анонсируемых сообщениях RA. Чтобы отключить флаг, воспользуйтесь формой **no** этой команды.

ipv6 nd other-config-flag
no ipv6 nd other-config-flag

Параметры

Нет.

По умолчанию

Данный функционал по умолчанию отключен.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Установив флаг O, маршрутизатор дает команду подключенным узлам использовать протокол конфигурации с отслеживанием состояния (Stateful Configuration), чтобы получить дополнительную информацию по автоматической конфигурации помимо IPv6-адреса.

Пример

В данном примере показано, как включить флаг O в сообщениях RA, анонсируемых в VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 nd other-config-flag
Switch(config-if)#
```

10.10 ipv6 nd prefix

Данная команда используется для настройки IPv6-префикса, который будет анонсироваться в сообщениях RA. Чтобы удалить префикс, воспользуйтесь формой **no** этой команды.

ipv6 nd prefix *IPV6-PREFIX/PREFIX-LENGTH* **[***VALID-LIFETIME PREFERRED-LIFETIME***] [off-link] [no-autoconfig]**

no ipv6 nd prefix *IPV6-PREFIX/PREFIX-LENGTH*

Параметры

IPV6-PREFIX	Укажите IPv6-префикс, который будет сгенерирован или анонсирован в сообщении RA на интерфейсе.
PREFIX-LENGTH	Укажите длину IPv6-префикса, который будет сгенерирован или анонсирован в сообщении RA на интерфейсе.
VALID-LIFETIME	(Опционально.) Укажите период времени в секундах, в течение которого префикс будет действителен. Диапазон значений: от 0 до 4294967295.
PREFERRED-LIFETIME	(Опционально.) Укажите предпочтительное время жизни префикса в секундах. Диапазон значений: от 0 до 4294967295.
off-link	(Опционально.) Укажите, чтобы отключить флаг наличия соединения on-link.
no-autoconfig	(Опционально.) Укажите, чтобы отключить флаг auto-configure.

По умолчанию

Значение *VALID-LIFETIME* по умолчанию – 2592000 секунд (30 дней).

Значение *PREFERRED-LIFETIME* по умолчанию – 604 800 секунд (7 дней).

Флаги on-link и auto-configure по умолчанию включены.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Значение допустимого времени жизни (Valid Lifetime) для префикса должно превышать значение предпочтительного времени жизни (Preferred Lifetime). Данные значения влияют на префикс, в котором включен бит A. Полученный узел будет конфигурировать адреса на основе префикса, используя механизм Stateless Configuration. Если время жизни префикса превысило значение предпочтительного времени (Preferred Lifetime), тогда IPv6-адрес, сконфигурированный на основе этого префикса, будет признан устаревшим. Если время жизни префикса превысило значение Valid Lifetime, то IPv6-адрес, сконфигурированный на основе этого префикса, будет удален.

Если IPv6-адрес настроен вручную на интерфейсе, соответствующий префикс будет анонсироваться автоматически. Анонсированный префикс может быть изменен, но не может быть удален с помощью данной команды. Если IPv6-адрес будет удален позже, анонсирование соответствующего префикса будет остановлено.

Пример

В данном примере показано, как настроить IPv6-префикс 3ffe:501:ffff:100::/64 с параметром Valid Lifetime продолжительностью 30000 секунд и Preferred Lifetime продолжительностью 20000 секунд.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 nd prefix 3ffe:501:ffff:100::/64 30000 20000
Switch(config-if)#
```

10.11 ipv6 nd ra interval

Данная команда используется для настройки временного интервала между сообщениями RA для IPv6-интерфейса. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 nd ra interval *MAX-SECS* **[***MIN-SECS***]**
no ipv6 nd ra interval

Параметры

MAX-SECS	Укажите максимальный временной интервал для повторной передачи сообщения RA (в секундах). Диапазон значений: от 4 до 1800 секунд.
MIN-SECS	(Опционально.) Укажите минимальный временной интервал для повторной передачи сообщения RA (в секундах). Это значение не должно превышать 0,75 максимального значения. Диапазон значений: от 3 до 1350 секунд.

По умолчанию

Максимальный временной интервал по умолчанию – 200 секунд.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Если минимальное значение временного интервала между сообщениями RA не настроено, к этому значению будут применяться следующие правила:

- Если максимальное значение интервала между сообщениями RA равно или превышает 9 секунд, то минимальный интервал должен составлять 33% от максимального значения.
- Если максимальное значение интервала между сообщениями RA меньше 9 секунд, минимальный и максимальный интервалы будут равны.

Пример

В данном примере показано, как задать временной интервал для сообщений RA IPv6.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 nd ra interval 1500 1000
Switch(config-if)#
```

10.12 ipv6 nd ra lifetime

Данная команда используется для настройки значения времени жизни (Lifetime) между сообщениями RA для IPv6-интерфейса. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 nd ra lifetime *SECONDS*
no ipv6 nd ra lifetime

Параметры

SECONDS	Укажите продолжительность использования маршрутизатора в качестве маршрутизатора по умолчанию (в секундах). Диапазон значений: от 0 до 9000.

По умолчанию

Значение по умолчанию – 1800 секунд.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Значение Lifetime в сообщении RA указывает узлу период времени, в течение которого маршрутизатор будет использоваться в качестве маршрутизатора по умолчанию.

Пример

В данном примере показано, как задать значение Lifetime в анонсируемых сообщениях RA. Указанное значение – 9000 секунд.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 nd ra lifetime 9000
Switch(config-if)#
```

10.13 ipv6 nd suppress-ra

Данная команда используется для отключения отправки сообщений RA на интерфейсе. Чтобы включить отправку сообщений RA, воспользуйтесь формой **no** этой команды.

ipv6 nd suppress-ra
no ipv6 nd suppress-ra

Параметры

Нет.

По умолчанию

По умолчанию функция включена на VLAN-интерфейсе.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов VLAN.

Используйте данную команду, чтобы отключить отправку сообщений RA на интерфейсе. Воспользуйтесь формой **no** этой команды для повторного включения отправки сообщений RA на интерфейсе.

Пример

В данном примере показано, как блокировать отправку сообщений RA для VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 nd suppress-ra
Switch(config-if)#
```

10.14 ipv6 nd reachable-time

Данная команда используется для настройки параметра Reachable Time (время доступности) в таблице ND-протокола. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 nd reachable-time *MILLI-SECONDS*
no ipv6 nd reachable-time

Параметры

MILLI-SECONDS	Укажите время доступности для отправляемых анонсов маршрутизатора (в миллисекундах). Диапазон значений: от 0 до 3600000, кратно 1000.

По умолчанию

Значение по умолчанию, анонсируемое в сообщениях RA, – 1200000.
Значение по умолчанию, используемое маршрутизатором, – 1200000 (1200 секунд).

Режим ввода команды

Interface Configuration Mode.

Использование команды

Заданное время используется маршрутизатором на интерфейсе и анонсируется в сообщении RA. Если задан 0, маршрутизатор будет использовать 30 секунд на интерфейсе и анонсировать 0 (не указано) в сообщении RA. Параметр Reachable Time используется IPv6-узлом для определения доступности соседних узлов.

Пример

В данном примере показано, как задать значение Reachable Time продолжительностью 3600 секунд для интерфейса VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch (config-if)# ipv6 nd reachable-time 3600000
Switch (config-if)#
```

10.15 ipv6 nd ns-interval

Данная команда используется для настройки временного интервала между повторными отправками сообщений NS. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ipv6 nd ns-interval *MILLI-SECONDS*
no ipv6 nd ns-interval

Параметры

MILLI-SECONDS	Укажите временной интервал отправки запросов NS (в миллисекундах). Диапазон значений: от 0 до 3600000 миллисекунд, кратно 1000.

По умолчанию

Значение по умолчанию, анонсируемое в сообщениях RA, – 0.
Значение по умолчанию, используемое маршрутизатором, – 1000 (1 секунда).

Режим ввода команды

Interface Configuration Mode.

Использование команды

Заданное время используется маршрутизатором на интерфейсе и анонсируется в сообщении RA. Если задан 0, маршрутизатор будет использовать 1 секунду на интерфейсе и анонсировать 0 (не указано) в сообщении RA.

Пример

В данном примере показано, как настроить отправку сообщений NS с интервалом 6 секунд.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch (config-if)# ipv6 nd ns-interval 6000
Switch (config-if)#
```

10.16 ipv6 neighbor

Данная команда используется для создания статической записи в таблице IPv6 neighbor. Для удаления статической записи из таблицы воспользуйтесь формой **no** этой команды.

ipv6 neighbor *IPV6-ADDRESS INTERFACE-ID MAC-ADDRESS*
no ipv6 neighbor *IPV6-ADDRESS INTERFACE-ID*

Параметры

IPV6-ADDRESS	Укажите IPv6-адрес для записи в IPv6 neighbor cache.
INTERFACE-ID	Укажите интерфейс для создания статической записи в IPv6 neighbor cache.
MAC-ADDRESS	Укажите MAC-адрес для записи в IPv6 neighbor cache.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду для создания статической записи в таблице IPv6 neighbor cache на интерфейсе. Статическая запись будет находиться либо в состоянии REACHABLE, если интерфейс включен, либо в состоянии INCOMPLETE, если интерфейс выключен. Отслеживание доступности соседних узлов к статическим записям не применяется.

Команда **clear ipv6 neighbors** позволяет удалять динамические записи из таблицы IPv6 neighbor. Для удаления статической записи воспользуйтесь командой **no ipv6 neighbor**.

Пример

В данном примере показано, как создать статическую запись в таблице IPv6 neighbor cache.

```
Switch# configure terminal
Switch(config)# ipv6 neighbor fe80::1 interface vlan 1 00-01-80-11-22-99
Switch(config)#
```

10.17 show ipv6 interface

Данная команда используется для отображения информации по IPv6-интерфейсу.

show ipv6 interface [*INTERFACE-ID***] [brief]**

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейс, для которого необходимо получить информацию.
brief	(Опционально.) Укажите, чтобы получить краткую информацию.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить настройки конфигурации IPv6-интерфейса.

Пример

В данном примере показано, как отобразить информацию по IPv6-интерфейсу.

```
Switch#show ipv6 interface vlan2

vlan2 is up, Link status is down
  IPv6 is enabled,
  link-local address:
      FE80::200:ABFF:FECD:1234
  Global unicast address:
      200::2/64 (Manual)
  RA messages are sent between 66 to 200 seconds
  RA advertised reachable time is 1200000 milliseconds
  RA advertised retransmit interval is 0 milliseconds
  RA advertised life time is 1800 seconds
  RA advertised O flag is OFF, M flag is OFF
  RA advertised prefixes
    200::/64
        valid lifetime is 2592000,  preferred lifetime is 604800

Total Entries: 1

Switch#
```

В примере ниже показано, как получить краткую информацию по IPv6-интерфейсу.

```
Switch# show ipv6 interface brief

vlan 1 is up, Link status is up
    FE80::201:1FF:FE02:304

vlan 2 is up, Link status is down
    FE80::201:1FF:FE02:305
    200::2

vlan 3 is up, Link status is down
    FE80::201:1FF:FE02:306

Total Entries: 3

Switch#
```

10.18 show ipv6 neighbors

Данная команда используется для отображения информации о соседних IPv6-устройствах.

show ipv6 neighbors [*INTERFACE-ID***] [***IPV6-ADDRESS***]**

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейс для отображения информации о записях в таблице IPv6 neighbor cache.
IPV6-ADDRESS	(Опционально.) Укажите IPv6-адрес, для которого необходимо получить информацию из таблицы IPv6 neighbor cache.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду для просмотра записи в таблице IPv6 neighbor cache.

Пример

В данном примере показано, как отобразить информацию о записях в таблице IPv6 neighbor cache.

```
Switch# show ipv6 neighbors

IPv6 Address                            Link-Layer Addr   Interface Type State
--------------------------------------- ----------------- --------- ---- -----
FE80::200:11FF:FE22:3344                00-00-11-22-33-44 vlan 1     D   REACH

Total Entries: 1

Switch#
```

Отображаемые параметры

Type	**D** – динамическая изученная запись. **S** – статическая neighbor-запись.
State	**INCMP** (неполное) – состояние, когда запрос на получение адреса для записи отправлен, но ответное сообщение neighbor advertisement еще не получено. **REACH** (достижимое) – состояние, когда сообщение neighbor advertisement уже получено, а время таймера Reachable Time (в миллисекундах) еще не истекло. Это означает, что соседнее устройство работает корректно. **STALE** – состояние, в которое переходит запись, если с момента получения последнего подтверждения прошло больше заданного таймером Reachable Time времени (в миллисекундах). **PROBE** – состояние записи, при котором устройство отправляет сообщение neighbor solicitation, чтобы подтвердить достижимость. **DELAY** – больше не известно, доступно ли соседнее устройство, которому недавно был отправлен трафик. Немедленная проверка с помощью отправки тестовых сообщений будет ненадолго отложена, чтобы дать возможность протоколам верхнего уровня подтвердить достижимость.

11. Команды Cable Diagnostics

11.1 test cable-diagnostics

Данная команда используется для запуска диагностики кабеля, чтобы проверить состояние и длину медного кабеля.

test cable-diagnostics interface *INTERFACE-ID* **[, | -]**

Параметры

interface *INTERFACE-ID*	Укажите ID интерфейса.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Команда используется для диагностики кабеля на физическом порту. Диагностика кабеля позволяет выявить проблемы с подключением на медных портах. Для запуска диагностики используйте команду **test cable-diagnostics**.

Пример

В данном примере показано, как запустить диагностику для проверки статуса и длины медного кабеля.

```
Switch#test cable-diagnostics interface eth1/0/1
Switch#
```

11.2 show cable-diagnostics

Данная команда используется для отображения результатов диагностики кабеля.

show cable-diagnostics [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите ID интерфейса.

,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта. Команда используется для отображения результатов диагностики кабеля.

Медный порт может находиться в одном из следующих состояний:

Open: пара в кабеле не имеет подключения в указанной позиции;

Short: короткое замыкание в кабеле в указанной позиции;

Open or Short: нет подключения или короткое замыкание, не удается определить тип неисправности;

Crosstalk: перекрестные помехи между парами в кабеле в указанной позиции;

Shutdown: удаленное устройство отключено;

Unknown: состояние неизвестно;

OK: неисправностей пары или кабеля не выявлено;

No cable: кабель не подключен к порту.

Пример

В данном примере показано, как отобразить результаты диагностики кабеля для интерфейса Ethernet 1/0/1.

```
Switch#show cable-diagnostics

Port      Type       Link Status   Test Result                 Cable Length (M)
--------- ---------- ------------ ------------------------- -----------------
eth1/0/1  10GBASE-T  Link Up       Pair 1 Open      at   2M  -
                                   Pair 2 OK        at   0M
                                   Pair 3 OK        at   0M
                                   Pair 4 Open      at   1M
eth1/0/2  10GBASE-T  Link Down     -                        -
eth1/0/3  10GBASE-T  Link Up       -                        -
eth1/0/4  10GBASE-T  Link Down     -                        -
eth1/0/5  10GBASE-T  Link Down     -                        -
eth1/0/6  10GBASE-T  Link Down     -                        -
eth1/0/7  10GBASE-T  Link Down     -                        -
eth1/0/8  10GBASE-T  Link Down     -                        -
eth1/0/9  10GBASE-T  Link Down     -                        -
eth1/0/10 10GBASE-T  Link Down     -                        -
eth1/0/11 10GBASE-T  Link Down     -                        -
eth1/0/12 10GBASE-T  Link Down     -                        -
eth1/0/13 10GBASE-T  Link Down     -                        -
eth1/0/14 10GBASE-T  Link Down     -                        -
eth1/0/15 10GBASE-T  Link Down     -                        -
eth1/0/16 10GBASE-T  Link Down     -                        -
eth1/0/17 10GBASE-T  Link Down     -                        -
eth1/0/18 10GBASE-T  Link Down     -                        -
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

11.3 clear cable-diagnostics

Данная команда позволяет удалить результаты диагностики кабеля.

clear cable-diagnostics {all | interface *INTERFACE-ID* **[, | -]}**

Параметры

all	Укажите, чтобы удалить результаты диагностики кабеля для всех интерфейсов.
interface *INTERFACE-ID*	Укажите ID интерфейса.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта. Используйте команду, чтобы удалить результаты диагностики кабеля на физическом порту. При выполнении диагностики на интерфейсе будет отображено сообщение об ошибке.

Пример

В данном примере показано, как удалить результаты диагностики кабеля.

```
Switch#clear cable-diagnostics interface eth1/0/1
Switch#
```

12. Команды Debug

12.1 debug enable

Данная команда используется для включения функции вывода сообщения отладки (Debug). Для отключения данной функции воспользуйтесь формой **no** этой команды.

debug enable
no debug enable

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы включить функцию вывода сообщения отладки (Debug).

Пример

В данном примере показано, как включить/выключить функцию вывода сообщения отладки (Debug).

```
Switch#configure terminal
Switch(config)#debug enable
Switch(config)#no debug enable
Switch(config)#
```

12.2 debug reboot on-error

Данная команда используется для включения режима перезапуска коммутатора при возникновении критических ошибок. Для отключения режима воспользуйтесь формой **no** этой команды.

debug reboot on-error
no debug reboot on-error

Параметры

Нет.

По умолчанию

По умолчанию данный режим включен.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду для включения режима перезапуска коммутатора при возникновении критических ошибок.

Пример

В данном примере показано, как включить режим перезапуска коммутатора при возникновении критических ошибок.

```
Switch#configure terminal
Switch(config)#debug reboot on-error
Switch(config)#
```

12.3 debug copy

Данная команда используется для копирования информации по отладке в указанный файл.

debug copy *SOURCE-URL DESTINATION-URL*
debug copy *SOURCE-URL* **{tftp:** *//LOCATION/DESTINATION-URL}*

Параметры

SOURCE-URL	Укажите ссылку на файл, который необходимо скопировать: **error-log:** укажите, чтобы скопировать данные журнала регистрации ошибок. **tech-support:** укажите, чтобы скопировать справочную техническую информацию. Можно скопировать только на TFTP-сервер.
DESTINATION-URL	Укажите URL-адрес назначения.
LOCATION	Укажите IPv4- или IPv6-адрес TFTP-сервера.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Использование команды

Используйте данную команду для копирования информации по отладке в указанный файл. Если скопирована информация **tech-support** и в стеке более одного коммутатора, будет сгенерировано несколько файлов, содержащих unit ID коммутатора в качестве суффикса в имени файла.

Пример

В данном примере показано, как скопировать данные буфера отладки на TFTP-сервер (10.90.90.99).

```
Switch#debug copy buffer tftp: //10.90.90.99/abc.txt

Address of remote host [10.90.90.99]?
Destination filename [abc.txt]?
 Accessing tftp://10.90.90.99/abc.txt...
Transmission starts...
Finished network upload(65739) bytes.

Switch#
```

12.4 debug clear error-log

Данная команда используется для очистки журнала регистрации ошибок.

debug clear error-log

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Использование команды

Используйте данную команду для очистки журнала регистрации ошибок.

Пример

В данном примере показано, как очистить журнал регистрации ошибок.

```
Switch#debug clear error-log
Switch#
```

12.5 debug show error-log

Данная команда используется для отображения данных журнала регистрации ошибок.

debug show error-log

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Использование команды

Используйте данную команду для отображения данных журнала регистрации ошибок.

Пример

В данном примере показано, как отобразить данные журнала регистрации ошибок.

```
Switch# debug show error-log

# debug log: 1
# level: fatal
# clock: 10000ms
# time : 2013/03/11 13:00:00
====================== SOFTWARE FATAL ERROR ======================
Invalid mutex handle : 806D6480

Current TASK : bcmARL.0
------------------------ TASK STACKTRACE -----------------------
->802ACE98
->8018C814
->8028FF44
->8028352C
->801D703C
->8013B8A4
->802AE754
->802A5E0C
->802A5D6C

*****************************************************************************
# debug log: 2
# level: fatal
# clock: 10000ms
# time : 2013/03/11 15:00:00
====================== SOFTWARE FATAL ERROR ======================
CLI_UTL_AllocateMemory Fail!

Current TASK : CLI
------------------------ TASK STACKTRACE -----------------------
->802ACE98
->802B4498
->802B4B00
->802BD140
->802BCB08

Total Log : 2

Switch#
```

12.6 debug show tech-support

Данная команда используется для отображения информации, запрашиваемой техническим персоналом.

debug show tech-support

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Использование команды

Используйте данную команду для отображения справочной технической информации. Эта информация используется для сбора данных о коммутаторе, необходимых инженерно-техническому персоналу для выявления и устранения неисправностей.

Пример

В данном примере показано, как отобразить данные технической поддержки всех модулей.

```
Switch#debug show tech-support

#------------------------------------------------------------------------------
#             DXS-1210-28T 10 Gigabit Ethernet Smart Managed Switch
#                          Technical Support Information
#
#                            Firmware: Build 1.00.021
#    Copyright(C) 2020  D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------------


********************   Basic System Information   ********************

[SYS 2019-1-1 07:33:49]

Boot Time           : 1 Jan 2019  00:00:00
RTC Time            : 2019/01/01 07:33:49
Bootloader Version  :
Linux Version       : 1.0.5
Runtime Version     : 1.00.021
Hardware Version    : A1
Serial number       : DXS1210102030
MAC Address         : F0-7D-68-12-10-01
MAC Address Number  : 65535

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

13. Команды DHCP Auto-Configuration

13.1 autoconfig enable

Данная команда используется для включения функции автоконфигурации. Для отключения данной функции воспользуйтесь формой **no** этой команды.

autoconfig enable
no autoconfig enable

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Если функция автоконфигурации включена, при перезапуске коммутатор автоматически становится DHCP-клиентом. Процесс автоконфигурации описан ниже:

- Коммутатор получает путь к файлу конфигурации, а также IP-адрес TFTP-сервера от DHCP-сервера (при наличии этих данных у DHCP-сервера, а также если в настройках указано, что DHCP-сервер может передавать данную информацию в поле данных пакета DHCP-ответа).
- Коммутатор загружает файл конфигурации, полученный от TFTP-сервера (если TFTP-сервер запущен и на момент получения запроса в его базовом каталоге присутствует необходимый файл конфигурации).

Если коммутатор не может завершить процесс автоконфигурации, будет использован прежде сохраненный локальный файл конфигурации.

Пример

В данном примере показано, как включить автоконфигурацию.

```
Switch# configure terminal
Switch(config)# autoconfig enable
Switch(config)#
```

13.2 show autoconfig

Данная команда используется для отображения статуса автоконфигурации.

show autoconfig

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для отображения статуса автоконфигурации.

Пример

В данном примере показано, как отобразить статус автоконфигурации.

```
Switch# show autoconfig

Autoconfig State: Disabled

Switch#
```

14. Команды DHCP Auto-Image

14.1 autoimage enable

Данная команда используется для включения функции Auto-Image. Для отключения данной функции воспользуйтесь формой **no** этой команды.

autoimage enable
no autoimage enable

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

При запуске коммутатора данная функция позволяет получить файл образа с внешнего TFTP-сервера, чей IP-адрес и имя файла содержатся в сообщении DHCP OFFER, полученном от DHCP-сервера. Полученный файл используется системой в качестве загрузочного. Если функция Auto-Image включена, при загрузке системы коммутатор автоматически становится DHCP-клиентом.

DHCP-клиент будет активирован для получения сетевых настроек от DHCP-сервера, который добавит в сообщение IP-адрес TFTP-сервера и имя файла образа. После получения данной информации коммутатор запустит функцию загрузки с указанного TFTP-сервера. На данном этапе в консоли будут отображены параметры конфигурации загрузки – так же, как при использовании команды **download firmware**.

После завершения загрузки программного обеспечения будет выполнена перезагрузка коммутатора.

Если одновременно включены функция Auto-Configuration и функция Auto-Image, сначала будет выполнена загрузка файла образа, а затем загрузка конфигурации. Коммутатор выполнит сохранение настроек, а затем – перезагрузку.

Полученное программное обеспечивание проходит проверку. Если версия нового программного обеспечения совпадает с версией текущего программного обеспечения, коммутатор завершит процесс Auto-Image. Однако если включена функция Auto-Configuration, загрузка конфигурации продолжится.

Функция Auto-Image аналогична функции Auto-Configuration. IP-адрес TFTP-сервера также размещен в полях siaddr DHCP Option 66 или Option 150. Если ответное DHCP-сообщение содержит одновременно поля Option 66, Option 150 и siaddr, сначала будет обработано поле Option 150. Если системе не удается подключиться к TFTP-серверу, будет обработано поле Option 66. Если подключиться снова не удается, будет обработано поле siaddr.

Если коммутатор использует Option 66 для получения имени TFTP-сервера, сначала будет обработано Option 6, что позволит получить IP-адрес DNS-сервера. Если коммутатору не удается подключиться к DNS-серверу или ответное сообщение не содержит Option 6, коммутатор попытается подключиться к DNS-серверу, уже установленному в системе вручную.

Так как поля DHCP Option используются не только в функции Auto-Image, но и в функции Auto-Configuration, файл образа и файл конфигурации должны быть размещены на одном TFTP-сервере.

При указании имени файла образа необходимо использовать DHCP Option 125 (RFC 3925). Коммутатор проверяет поле enterprise-number1. Если его значение не совпадает с указанным D-Link Vendor ID (171), процесс будет остановлен. При наличии нескольких данных будут использоваться только первые данные enterprise-number1.

Пример

В данном примере показано, как включить функцию Auto-Image.

```
Switch#configure terminal
Switch(config)#autoimage enable
Switch(config)#
```

14.2 autoimage timeout

Данная команда используется для указания тайм-аута, в течение которого будет получен файл образа.

autoimage timeout *SECONDS*

Параметры

SECONDS	Укажите тайм-аут в диапазоне от 1 до 65535 секунд.

По умолчанию

Значение по умолчанию – 50 секунд.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы указать тайм-аут, в течение которого будет получен файл образа.

Пример

В данном примере показано, как настроить тайм-аут 60 секунд.

```
Switch#configure terminal
Switch(config)#autoimage timeout 60
Switch(config)#
```

14.3 show autoimage

Данная команда используется для отображения статуса Auto-Image.

show autoimage

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить статус Auto-Image.

Пример

В данном примере показано, как отобразить статус Auto-Image.

```
Switch#show autoimage

Autoimage State: Disabled
Timeout        : 60

Switch#
```

15. Команды DHCP Client

15.1 ip dhcp client class-id

Данная команда используется для указания Vendor Class Identifier, используемого в качестве значения Option 60 для сообщения DHCP Discover. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip dhcp client class-id {*MULTI-WORD* **| hex** *HEX-STRING***}**
no ip dhcp client class-id

Параметры

MULTI-WORD	Укажите Vendor Class Identifier в формате строки. Максимальная длина строки – 32 символа.
hex *HEX-STRING*	Укажите Vendor Class Identifier в шестнадцатеричном формате. Максимальная длина строки – 64 символа.

По умолчанию

По умолчанию в качестве ID класса используется тип устройства.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Используйте данную команду для обозначения Vendor Class Identifier (Option 60), который необходимо отправить в сообщении DHCP Discover. Данная функция применима только для последующей отправки сообщений DHCP Discover. Данная функция работает, когда на интерфейсе включен DHCP-клиент, который может получить IP-адрес от DHCP-сервера. Vendor Class Identifier определяет тип устройства, запрашивающего IP-адрес.

Пример

В данном примере показано, как указать значение «VOIP Device» в качестве Vendor Class Identifier для VLAN 100 и настроить отправку Vendor Class Identifier в сообщении DHCP Discover.

```
Switch#configure terminal
Switch(config)#interface vlan 100
Switch(config-if)#ip address dhcp
Switch(config-if)#ip dhcp client class-id VOIP-Device
Switch(config-if)#
```

15.2 ip dhcp client client-id

Данная команда используется для обозначения интерфейса VLAN, шестнадцатеричный MAC-адрес которого будет использован в качестве ID клиента, отправляемого в сообщении Discover. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip dhcp client client-id *INTERFACE-ID*
no ip dhcp client client-id

Параметры

INTERFACE-ID	Укажите интерфейс VLAN, шестнадцатеричный MAC-адрес которого будет использован в качестве ID клиента и отправлен в сообщении Discover.

По умолчанию

По умолчанию в качестве ID клиента используется MAC-адрес VLAN.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Используйте данную команду для настройки шестнадцатеричного MAC-адреса обозначенного интерфейса в качестве ID клиента, отправляемого в сообщении Discover. Данная функция применима только для последующей отправки сообщений DHCP Discover. Данная функция работает, когда на интерфейсе включен клиент DHCP, который может получить IP-адрес от сервера DHCP. Идентификатором клиента может быть назначен один интерфейс.

Пример

В данном примере показано, как сконфигурировать MAC-адрес VLAN 100 в качестве ID клиента, отправляемого в сообщении Discover для VLAN 100.

```
Switch#configure terminal
Switch(config)#interface vlan 100
Switch(config-if)#ip dhcp client client-id vlan 100
Switch(config-if)#
```

15.3 ip dhcp client lease

Данная команда используется для указания времени аренды IP-адреса, который необходимо запросить у DHCP-сервера. Для отключения данной функции воспользуйтесь формой **no** этой команды.

ip dhcp client lease *DAYS* **[***HOURS* **[***MINUTES***]]**

no ip dhcp client lease

Параметры

DAYS	Укажите продолжительность аренды в днях. Допустимый диапазон: от 0 до 10000 дней.
HOURS	(Опционально.) Укажите продолжительность аренды в часах. Допустимый диапазон: от 0 до 23 часов.
MINUTES	(Опционально.) Укажите продолжительность аренды в минутах. Допустимый диапазон: от 0 до 59 минут.

По умолчанию

Время аренды не запрашивается.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная функция работает, если DHCP-клиент может запросить IP-адрес для интерфейса.

Пример

В данном примере показано, как получить аренду IP-адреса на пять дней.

```
Switch#configure terminal
Switch(config)#interface vlan 100
Switch(config-if)#ip address dhcp
Switch(config-if)#ip dhcp client lease 5
Switch(config-if)#
```

16. Команды DHCP Relay

16.1 class (DHCP relay)

Данная команда используется для входа в режим DHCP Pool Configuration Mode и привязки диапазона IP-адресов к DHCP-классу. Для удаления привязки воспользуйтесь формой **no** этой команды.

class *NAME*
no class *NAME*

Параметры

NAME	Укажите имя DHCP-класса. Максимальная длина – 32 символа.

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Configuration Mode.

Использование команды

Данная команда применяется для привязки пула DHCP relay pool к DHCP pool class. Используйте команду **relay target**, чтобы указать список адресов relay target для перенаправления DHCP-пакета. Если запрос DHCP-клиента совпадает с пулом relay, настроенным с классами, клиент должен соответствовать классу, настроенному в пуле, для ретрансляции. Если DHCP-класс не настроен, запрос будет сопоставляться только с пулом relay и будет ретранслироваться на сервер назначения relay, указанный для соответствующего пула relay.

Пример

В данном примере показано, как настроить DHCP-класс, «Service-A», определенный шаблоном соответствия DHCP Option 60 в виде 0x112233 и 0x102030, классифицированным для пула relay, «pool1», и связанный с relay target «10.2.1.2».

```
Switch# configure terminal
Switch(config)#ip dhcp class Service-A
Switch(config-dhcp-class)#option 60 hex 112233
Switch(config-dhcp-class)#option 60 hex 102030
Switch(config-dhcp-class)#exit
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#relay source 172.19.18.0 255.255.255.0
Switch(config-dhcp-pool)#class Service-A
Switch(config-dhcp-pool-class)#relay target 10.2.1.2
Switch(config-dhcp-pool-class)#
```

16.2 ip dhcp class (DHCP relay)

Данная команда используется для указания DHCP-класса и входа в режим DHCP Class Configuration Mode. Для удаления DHCP-класса воспользуйтесь формой **no** этой команды.

ip dhcp class *NAME*
no ip dhcp class *NAME*

Параметры

NAME	Укажите имя DHCP-класса, содержащее не более 32 символов в длину.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду для входа в режим DHCP Class Configuration Mode и команду **option hex** для указания шаблона соответствия для DHCP-класса. Если у класса нет связанной с ним шестнадцатеричной опции, то классу будет соответствовать любой пакет.

Пример

В данном примере показано, как настроить DHCP-класс Service-A и указать шаблон соответствия DHCP Option 60 в виде 0x112233.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-A
Switch(config-dhcp-class)#option 60 hex 112233
Switch(config-dhcp-class)#
```

16.3 ip dhcp pool (DHCP Relay)

Данная команда используется для настройки пула DHCP Relay на DHCP Relay Agent и входа в режим DHCP Pool Configuration Mode. Для удаления пула DHCP Relay воспользуйтесь формой **no** данной команды.

ip dhcp pool *NAME*
no ip dhcp pool *NAME*

Параметры

NAME	Укажите имя пула адресов. Максимальное количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Наряду с пакетами DHCP Relay, Relay Destination DHCP-сервера можно указать в пуле DHCP Relay. Для этого войдите в режим настройки пула DHCP с помощью команды **ip dhcp pool**, затем при помощи команды **relay source** укажите подсеть-источник (source) запросов клиента, далее при помощи команды **relay destination** укажите адрес Relay Destination Server.

Если подсеть, от которой приходит пакет DHCP-запроса, соответствует Relay Source Relay-пула, пакет будет ретранслирован на основе данного пула. Чтобы ретранслировать пакет на основе пула DHCP Relay, если пакет запроса является ретранслируемым пакетом, источником запроса должен быть GIADDR (IP-адрес шлюза) пакета. Если GIADDR является нулевым, подсеть полученного интерфейса является источником пакета.

В пуле DHCP Relay администратор может далее использовать команды **class** и **relay target**, чтобы определить адрес Relay Target для пакетов запроса, который соответствует шаблону опции.

Пример

В данном примере показано, как создать пул DHCP Relay. Имя пула – pool1. Подсеть-источник (source) – 172.19.18.0/255.255.255.0. Адрес Relay Destination – 10.2.1.1.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#relay source 172.19.18.0 255.255.255.0
Switch(config-dhcp-pool)#relay destination 10.2.1.1
Switch(config-dhcp-pool)#
```

16.4 ip dhcp relay information check

Данная команда позволяет включить в DHCP Relay Agent проверку/удаление информации Relay Agent Information Option (Option 82) в полученном пакете DHCP-ответа. Для глобального отключения функции Check для Option 82 воспользуйтесь формой **no** этой команды.

ip dhcp relay information check
no ip dhcp relay information check

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда применима, если включен сервис DHCP.
Команды **ip dhcp relay information check** и **ip dhcp relay information check-reply** используются для определения эффективности функции Check Option 82 для интерфейса. Если на интерфейсе не настроена команда **ip dhcp relay information check-reply**, будут применены общие настройки. Если

на интерфейсе настроена команда **ip dhcp relay information check-reply**, будут применены настройки интерфейса.

После запуска функции Check для Option 82 ответного пакета устройство проверит пригодность поля Option 82 в пакетах DHCP-ответа, получаемых от DHCP-сервера. Если в получаемом пакете отсутствует поле Option 82 или опция не является оригинальной опцией, встроенной агентом (агент встраивает sub-опцию Remote ID при проверке), то Relay Agent отбрасывает пакет. В противном случае Relay Agent удаляет поле Option 82 и передает пакет.

Если функция Check отключена, пакет будет передан напрямую.

Пример

В данном примере показано глобальное включение функции Check DHCP Relay Agent.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information check
Switch(config)#
```

16.5 ip dhcp relay information check-reply

Данная команда используется для настройки в DHCP Relay Agent проверки информации Relay Agent Information Option (Option 82) в полученном пакете DHCP-ответа. Для удаления данных настройки для интерфейса воспользуйтесь формой **no** этой команды.

ip dhcp relay information check-reply [none]

no ip dhcp relay information check-reply [none]

Параметры

none	(Опционально.) Укажите, чтобы отключить функцию Check для Option 82 ответного пакета.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима, если включен сервис DHCP.

Команды **ip dhcp relay information check** и **ip dhcp relay information check-reply** используются для определения эффективности функции Check Option 82 для интерфейса. Если на интерфейсе не настроена команда **ip dhcp relay information check-reply**, будут применены общие настройки. Если на интерфейсе настроена команда **ip dhcp relay information check-reply**, будут применены настройки интерфейса.

После запуска функции Check для Option 82 ответного пакета устройство проверит пригодность поля Option 82 в пакетах DHCP-ответа, получаемых от DHCP-сервера. Если в получаемом пакете отсутствует поле Option 82, или опция не является оригинальной опцией, встроенной агентом (агент встраивает sub-опцию Remote ID при проверке), Relay Agent отбрасывает пакет. В противном случае Relay Agent удаляет поле Option 82 и передает пакет.

Если проверка отключена, пакет будет передан напрямую.

Пример

В данном примере показано, как глобально отключить функцию Check DHCP Relay Agent и включить функцию Check для VLAN 100. Включен рабочий режим функции Check для VLAN 100.

```
Switch# configure terminal
Switch(config)# no ip dhcp relay information check
switch(config)# interface vlan 100
switch(config-if)# ip dhcp relay information check-reply
```

16.6 ip dhcp relay information option

Данная команда используется, чтобы глобально включить вставку информации о Relay Agent (Option 82) в ретранслируемых пакетах DHCP-запроса. Для отключения данной функции воспользуйтесь формой **no** этой команды.

ip dhcp relay information option
no ip dhcp relay information option

Параметры

Нет.

По умолчанию

По умолчанию Option 82 не встроена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда действует при включенной команде **service dhcp**.

Если Option 82 DHCP включена, то перед ретрансляцией на сервер в пакет DHCP, получаемый от клиента, будет встроено поле Option 82. Option 82 DHCP содержит две sub-опции: Circuit ID и Remote ID.

Администраторы могут использовать команду **ip dhcp relay information option remote-id**, чтобы указать строку, заданную пользователем для sub-опции remote ID.

Пример

В данном примере показано, как встроить Option 82 в ретранслируемые пакеты DHCP-запроса.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information option
Switch(config)#
```

16.7 ip dhcp relay information option-insert

Данная команда используется для включения и настройки встраивания Option 82 в ретранслируемые пакеты DHCP-запроса на указанном интерфейсе. Для удаления настроек данной функции воспользуйтесь формой **no** этой команды.

ip dhcp relay information option-insert [none]

no ip dhcp relay information option-insert [none]

Параметры

none	(Опционально.) Укажите, чтобы отключить встраивание Option 82 в ретранслируемый пакет.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима, если запущена команда **service dhcp**.
Данная команда применима исключительно для настройки интерфейсов VLAN.
Используйте данную команду, чтобы настроить встраивание Option 82 в ретранслируемые пакеты DHCP-ответа на указанном интерфейсе. Если команда не сконфигурирована, будут действовать настройки команды **ip dhcp relay information option**.

Пример

В данном примере показано, как включить функцию встраивания Option 82 в ретранслируемые пакеты DHCP-ответа и выключить данную функцию для интерфейса VLAN 100. Функция встраивания Option 82 выключена для VLAN 100, но включена для оставшихся интерфейсов.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information option
Switch(config)#interface vlan 100
Switch(config-if)#ip dhcp relay information option-insert none
Switch(config-if)#
```

16.8 ip dhcp relay information policy

Данная команда используется для глобальной настройки алгоритма перенаправления Option 82 для DHCP Relay Agent. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip dhcp relay information policy {drop | keep | replace}

no ip dhcp relay information policy

Параметры

drop	Укажите, чтобы отбросить пакет, у которого уже есть Relay Option.
keep	Укажите, чтобы напрямую в неизменном виде отправить пакет DHCP-запросов, у которого уже есть Relay Option, на DHCP-сервер.
replace	Укажите, чтобы заменить пакет DHCP-запросов, у которого уже есть Relay Option, новой опцией.

По умолчанию

Параметр по умолчанию – **replace**.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда действует при включенной команде **service dhcp**.
Используйте данную команду для настройки общего алгоритма встраивания Option 82 в пакеты, у которых уже есть Option 82.

Пример

В данном примере показано, как настроить алгоритм перенаправления Relay Agent Option (Option 82) с помощью параметра keep.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information policy keep
Switch(config)#
```

16.9 ip dhcp relay information policy-action

Данная команда используется, чтобы настроить алгоритм перенаправления Option 82 для DHCP Relay Agent на интерфейсе. Для отмены конфигурации воспользуйтесь формой **no** этой команды.

ip dhcp relay information policy-action {drop | keep | replace}

no ip dhcp relay information policy-action

Параметры

drop	Укажите, чтобы отбросить пакет, у которого уже есть Relay Option.
keep	Укажите, чтобы в неизменном виде отправить пакет DHCP-запросов, у которого уже есть Relay Option, напрямую на DHCP-сервер.
replace	Укажите, чтобы заменить пакет DHCP-запросов, у которого уже есть Relay Option, новой опцией.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда действует, если запущена команда **service dhcp**.
Данная команда применима исключительно для настройки интерфейсов VLAN.
Используйте данную команду, чтобы настроить политику перенаправления для DHCP Relay Agent на указанном интерфейсе. Если команда не сконфигурирована, будут действовать настройки команды **ip dhcp relay information policy**.

Пример

В данном примере показано, как настроить алгоритм перенаправления Relay Agent Option с помощью параметра keep, а также как настроить соответствующий алгоритм для VLAN 100 с помощью параметра drop. Для VLAN 100 эффективным алгоритмом перенаправления Relay Agent Option является drop, для других интерфейсов – keep.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information policy keep
Switch(config)#interface vlan 100
Switch(config-if)#ip dhcp relay information policy-action drop
Switch(config-if)#
```

16.10 ip dhcp relay information option format remote-id

Данная команда используется для настройки sub-опции Remote ID DHCP. Для применения настроек по умолчанию воспользуйтесь формой **no** этой команды.

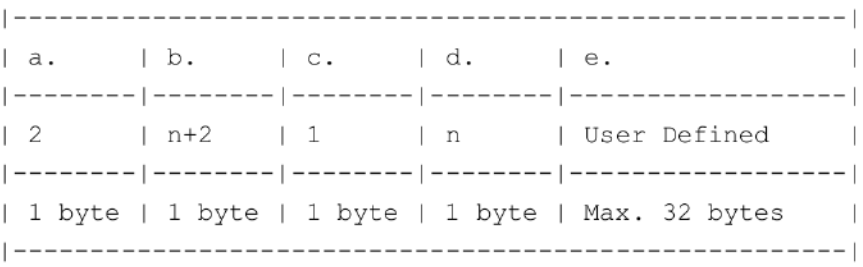
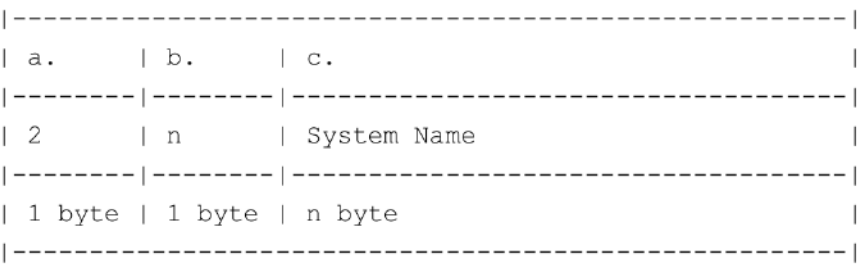
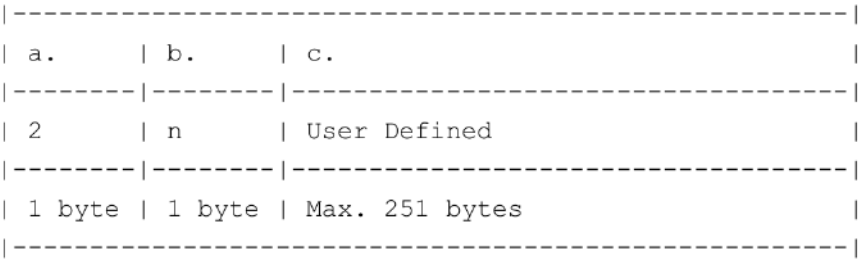
ip dhcp relay information option format remote-id {default| string *SENTENCE* **| vendor2 | vendor3}**

no ip dhcp relay information option format remote-id

Параметры

default	Укажите, чтобы использовать системный MAC-адрес коммутатора в качестве Remote ID. Формат Remote ID представлен ниже:

a.	b.	c.	d.	e.
2	8	0	6	MAC Address
1 byte	1 byte	1 byte	1 byte	6 bytes

string *SENTENCE*	Укажите, чтобы задать Remote ID самостоятельно. Допустимо использование пробелов. Формат Remote ID представлен ниже:  | a. | b. | c. | d. | e. | | 2 | n+2 | 1 | n | User Defined | | 1 byte | 1 byte | 1 byte | 1 byte | Max. 32 bytes |
vendor2	Укажите, чтобы использовать vendor 2. Оригинальный формат Remote ID представлен ниже:  | a. | b. | c. | | 2 | n | System Name | | 1 byte | 1 byte | n byte | **a.** *Тип sub-опции*: число 2 указывает, что это remote ID. **b**. *Длина*: длина значения. **c**. *Значение*: строка символов. Системное имя коммутатора.
vendor3	Укажите, чтобы использовать vendor 3. Оригинальный формат Remote ID представлен ниже:  | a. | b. | c. | | 2 | n | User Defined | | 1 byte | 1 byte | Max. 251 bytes | **a.** *Тип sub-опции*: число 2 указывает, что это remote ID. **b**. *Длина*: общая длина строки, задаваемой пользователем. По умолчанию длина равна 0, поле значений отсутствует. **c**. *Значение*: универсальная задаваемая пользователем строка, настраиваемая при помощи команды **ip dhcp relay information option format-type remote-id vendor3 string** *STRING*. Максимальная длина строки – 32 символа.

По умолчанию

По умолчанию в качестве строки Remote ID используется системный MAC-адрес коммутатора.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для выбора различных vendor-ов или заданной пользователем строки ASCII в качестве Remote ID.

Пример

В данном примере показано, как настроить vendor2 в качестве Remote ID.

```
Switch# Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format remote-id vendor2
Switch(config)#
```

В примере ниже показано, как настроить в качестве Remote ID строку, задаваемую пользователем. В примере используется строка «switch1».

```
Switch#configure terminal
Switch(config)#ip dhcp relay information option
Switch(config)#ip dhcp relay information option format remote-id string switch1
Switch(config)#
```

16.11 ip dhcp relay information option format-type remote-id

Данная команда используется для настройки sub-опции Remote ID DHCP как строки формата vendor в режиме Interface Configuration Mode. Для удаления sub-опции Remote ID как строки формата vendor воспользуйтесь формой **no** этой команды.

ip dhcp relay information option format-type remote-id vendor3 string *STRING*
no ip dhcp relay information option format-type remote-id vendor3

Параметры

vendor3	Укажите строку vendor 3, задаваемую пользователем. Максимальная длина строки – 32 символа.
STRING	Укажите строку, задаваемую пользователем.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Команда применима исключительно для настройки интерфейсов физического порта и port-channel.

Используйте данную команду для настройки строки, определенной как vendor для sub-опции Remote ID Option 82 на интерфейсе.

Пример

В данном примере показано, как настроить строку формата vendor 3 remote-id для интерфейса Ethernet 1/0/3. В примере используется строка «switch1».

```
Switch# configure terminal
Switch(config)# interface eth1/0/3
Switch(config-if)# ip dhcp relay information option format-type remote-id vendor3 string
switch1
Switch(config-if)#
```

16.12 ip dhcp relay information option format circuit-id

Данная команда используется для настройки sub-опции Circuit ID DHCP. Для применения настроек по умолчанию воспользуйтесь формой **no** этой команды.

ip dhcp relay information option format circuit-id {default | string *SENTENCE* **| vendor1 | vendor2 | vendor3 | vendor4 | vendor5 | vendor6}**

no ip dhcp relay information option format circuit-id

Параметры

default	Укажите, чтобы использовать sub-опцию Circuit ID по умолчанию. Оригинальный формат Circuit ID представлен ниже:

a.	b.	c.	d.	e.	f.	g.
1	0x6	0	4	VLAN	Module ID	Port ID
1 byte	1 byte	1 byte	1 byte	2 bytes	1 byte	1 byte

a. *Тип sub-опции*: число 1 свидетельствует о том, что тип данного ID – Circuit ID.

b. *Длина*: длина значения. Необходимая длина значения – 6.

c. *Sub-опция Circuit ID*: необходимое значение – 0.

d. *Длина sub-опции*: необходимое значение – 4.

e. *VLAN ID (S-VID).*

f. *ID модуля*: необходимое значение для автономных коммутаторов – 0.

g. *ID порта*: номер порта для каждого Unit ID.

string *SENTENCE*	Укажите, чтобы задать Circuit ID самостоятельно. Допустимо использование пробелов. |----------|----------|----------|----------|----------| | a. | b. | c. | d. | e. | |----------|----------|----------|----------|----------| | 2 | n+2 | 1 | n | User Defined | |----------|----------|----------|----------|----------| | 1 byte | 1 byte | 1 byte | 1 byte | Max. 32 bytes | |----------|----------|----------|----------|----------|
vendor1	Формат Circuit ID представлен ниже: |----------|----------|----------|----------|----------|----------| | a. | b. | c. | d. | e. | f. | |----------|----------|----------|----------|----------|----------| | 1 | 0x10 | 0 | 6 | VLAN | Slot ID | |----------|----------|----------|----------|----------|----------| | 1 byte | 1 byte | 1 byte | 1 byte | 2 bytes | 2 bytes | |----------|----------|----------|----------|----------|----------| |----------|----------|----------|----------| | g. | h. | i. | j | |----------|----------|----------|----------| | Port ID | 1 | 6 | MAC | |----------|----------|----------|----------| | 2 bytes | 1 byte | 1 byte | 6 bytes | |----------|----------|----------|----------| **a.** *Тип sub-опции*: число 1 свидетельствует о том, что тип данного ID – Circuit ID. **b**. *Длина*. **c**. *Первый тег sub-опции Circuit ID*: необходимое значение – 0. **d.** *Длина первого тега:* необходимое значение – 6. **e.** *VLAN ID*. **f**. *ID слота*: необходимое значение для автономных коммутаторов – 1. **g**. *ID порта*: номер порта для каждого Unit ID. **h.** *Второй тег sub-опции Circuit ID*: необходимое значение – 1. **i**. *Длина второго тега*: необходимое значение – 6. **j**. *MAC-адрес*: системный MAC-адрес коммутатора.
vendor2	Укажите, чтобы использовать vendor2.
vendor3	Укажите, чтобы использовать vendor3.
vendor4	Укажите, чтобы использовать vendor4.
vendor5	Укажите, чтобы использовать vendor5.

vendor6	Укажите, чтобы использовать vendor6.

По умолчанию

По умолчанию форматом Circuit ID являются ID VLAN, номер модуля и номер порта.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для выбора различных vendor-ов или заданной пользователем строки ASCII в качестве Circuit ID.

Пример

В данном примере показано, как использовать vendor1 в качестве Circuit ID.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information option
Switch(config)#ip dhcp relay information option format circuit-id vendor1
Switch(config)#
```

В примере ниже показано, как настроить в качестве Circuit ID строку, задаваемую пользователем. В примере используется строка «abcd».

```
Switch#configure terminal
Switch(config)#ip dhcp relay information option
Switch(config)#ip dhcp relay information option format circuit-id string abcd
Switch(config)#
```

16.13 ip dhcp relay information option format-type circuit-id

Данная команда используется для настройки Circuit ID Option 82 в строке, задаваемой пользователем, для различных вендоров на указанном интерфейсе. Для удаления Circuit ID Option 82 воспользуйтесь формой **no** этой команды.

ip dhcp relay information option format-type circuit-id vendor3 string *STRING*
no ip dhcp relay information option format-type circuit-id vendor3 string

Параметры

vendor3	Укажите строку vendor3, задаваемую пользователем. Максимальное количество символов – 32.
STRING	Укажите строку, задаваемую вендором.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и port-channel.

Используйте данную команду для настройки Circuit ID Option 82 в строке, задаваемой пользователем, для различных вендоров на указанном интерфейсе.

Пример

В данном примере показано, как настроить vendor3 «abc» для интерфейса Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)# ip dhcp relay information option format-type circuit-id vendor3 string abc
Switch(config-if)#
```

16.14 ip dhcp relay information trust-all

Данная команда позволяет назначить на DHCP Relay Agent все интерфейсы, отправляющие информацию об IP DHCP Relay, доверенными. Для отключения функции Trust для всех интерфейсов воспользуйтесь формой **no** этой команды.

ip dhcp relay information trust-all

no ip dhcp relay information trust-all

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Если на интерфейсе включена опция Trust для информации IP DHCP Relay, будут приниматься пакеты, GIADDR которых равен 0 (данный Relay Agent является первой ретрансляцией данного пакета DHCP-запроса), но у которых присутствует Relay Agent Information Option (Option 82). Если интерфейс не является доверенным, пакеты будут отброшены.

Если применены настройки данной команды, информация IP DHCP Relay является доверенной со всех интерфейсов. Если настройки данной команды не применены, статус информации определяется командой **ip dhcp relay information trusted** в режиме интерфейса.

Проверить настройки можно при помощи команды **show ip dhcp relay information trusted-sources**.

Пример

В данном примере показано, как назначить на DHCP Relay Agent информацию IP DHCP Relay в качестве доверенной со всех интерфейсов.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information trust-all
Switch(config)#
```

16.15 ip dhcp relay information trusted

Данная команда позволяет назначить на DHCP Relay Agent определенный интерфейс, отправляющий информацию об IP DHCP Relay, в качестве доверенного. Для отключения функции Trust воспользуйтесь формой **no** этой команды.

ip dhcp relay information trusted
no ip dhcp relay information trusted

Параметры

Нет.

По умолчанию

По умолчанию информация не является доверенной.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Если информация IP DHCP Relay отправляется с доверенного интерфейса, будут приниматься пакеты, GIADDR которых равен 0 (данный Relay Agent является первой ретрансляцией данного пакета DHCP-запроса), но у которых присутствует Relay Agent Information Option (Option 82). Если интерфейс не является доверенным, пакеты будут отброшены.

Если применены настройки команды **ip dhcp relay information trust-all**, информация IP DHCP Relay является доверенной со всех интерфейсов. Если настройки данной команды не применены, статус информации определяется командой **ip dhcp relay information trusted** в режиме интерфейса.

Проверить настройки можно при помощи команды **show ip dhcp relay information trusted-sources**.

Пример

В данном примере показано, как снять статус trust для всех интерфейсов на DHCP Relay Agent и запустить статус trust для VLAN 100.

```
Switch#configure terminal
Switch(config)#no ip dhcp relay information trust-all
Switch(config)#interface vlan 100
Switch(config-if)#ip dhcp relay information trusted
Switch(config-if)#
```

16.16 ip dhcp local-relay vlan

Данная команда используется для включения Local Relay на одной из VLAN или группе VLAN. Для отключения данной функции воспользуйтесь формой **no** этой команды.

ip dhcp local-relay vlan *VLAN-ID* **[, | -]**
no ip dhcp local-relay vlan *VLAN-ID* **[, | -]**

Параметры

VLAN-ID	Укажите используемую VLAN.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Local Relay обеспечивает передачу сообщения DHCP на все локальные member-порты VLAN на основе настроек Relay Option. Local Relay не изменяет IP-адрес и MAC-адрес назначения, а также поле шлюза пакета.

Пример

В данном примере показано, как включить функцию Local Relay на VLAN 100.

```
Switch#configure terminal
Switch(config)#ip dhcp local-relay vlan 100
Switch(config)#
```

16.17 option hex (DHCP relay)

Данная команда используется, чтобы указать шаблон соответствия DHCP option для DHCP-класса. Для удаления указанного шаблона соответствия для DHCP-класса воспользуйтесь формой **no** этой команды.

option *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**
no option *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**

Параметры

CODE	Укажите номер DHCP option.

PATTERN	Укажите шестнадцатеричный шаблон определенной DHCP option.
*	(Опционально.) Укажите биты опции, которые не будут проверяться на соответствие. Если параметр * не указан, количество битов шаблона должно быть таким же, что и количество битов опции.
MASK	(Опционально.) Укажите шестнадцатеричную битовую маску для шаблона. Биты маски шаблона будут соответствующими. Если маска не указана, все биты, указанные шаблоном, будут проверены. Будет проверен бит со значением FF. Формат ввода должен быть таким же, как и у шаблона.

По умолчанию

Нет.

Режим ввода команды

DHCP Class Configuration Mode.

Использование команды

Пользователь может использовать команду **ip dhcp class** наряду с командой **option hex**, чтобы указать DHCP-класс. Классы в пуле распределяются в том порядке, в котором они настроены в пуле адресов.

Команда **option hex** применяется для указания номера DHCP-опции с шаблоном соответствия для DHCP-класса. Для одного DHCP-класса можно указать несколько шаблонов опции. Если пакет соответствует какому-либо из указанных шаблонов DHCP-класса, он будет причислен к DHCP-классу и передан в указанное место назначения

Ниже приведены некоторые часто используемые номера опций:

- Option 60 (Vendor Class Identifier);
- Option 61 (Client Identifier);
- Option 77 (User Class);
- Option 124 (Vendor-identifying Vendor Class);
- Option 125 (Vendor-identifying Vendor-specific Information).

Пример

В данном примере показано, как настроить DHCP-класс Service-A с шаблоном соответствия DHCP Option 60 в виде 0x112233 и 0x102030.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-A
Switch(config-dhcp-class)#option 60 hex 112233
Switch(config-dhcp-class)#option 60 hex 102030
Switch(config-dhcp-class)#
```

16.18 relay destination

Данная команда используется для указания IP-адреса назначения DHCP Relay Destination, ассоциированного с пулом Relay. Для удаления Relay Destination из пула DHCP Relay воспользуйтесь формой **no** этой команды.

relay destination *IP-ADDRESS*
no relay destination *IP-ADDRESS*

Параметры

IP-ADDRESS	Укажите IP-адрес DHCP Relay Destination Server.

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Configuration Mode.

Использование команды

Relay Destination DHCP-сервера можно указать в пуле DHCP Relay. Для этого войдите в режим настройки пула DHCP при помощи команды **ip dhcp pool**, далее при помощи команды **relay source** укажите подсеть-источник (source) запросов клиента. После чего с помощью команды **relay destination** укажите адрес Relay Destination Server. В пуле можно указать несколько адресов Relay Source и Relay Destination. Если пакет соответствует какому-либо из адресов Relay Source, он будет отправлен на все адреса Relay Destination.

Если подсеть, от которой приходит пакет DHCP-запроса, соответствует Relay Source Relay-пула, пакет будет ретранслирован на основе данного пула. Чтобы ретранслировать пакет на основе пула DHCP Relay, если пакет запроса является ретранслируемым пакетом, источником запроса должен быть GIADDR (IP-адрес шлюза) пакета. Если пакет запроса не является ретранслируемым пакетом, источником пакета является подсеть получающего интерфейса.

В пуле DHCP Relay администратор может далее использовать команды **class** и **relay target**, чтобы связать список адресов Relay Target с классом DHCP.

Пример

В данном примере показано, как создать пул DHCP Relay под именем «pool1». В Relay-пуле подсеть 172.19.10.0/255.255.255.0 указана в качестве подсети-источника (source), а 10.2.1.1 указан в качестве адреса Relay Destination.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#relay source 172.19.10.0 255.255.255.0
Switch(config-dhcp-pool)#relay destination 10.2.1.1
Switch(config-dhcp-pool)#
```

16.19 relay source

Данная команда используется для указания подсети-источника (source) пакетов клиента. Для удаления подсети-источника воспользуйтесь формой **no** этой команды.

relay source *IP-ADDRESS SUBNET-MASK*
no relay source *IP-ADDRESS SUBNET-MASK*

Параметры

IP-ADDRESS	Укажите исходную подсеть-источник (source) пакетов клиента.
SUBNET-MASK	Укажите маску подсети-источника (source).

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Configuration Mode.

Использование команды

Relay Destination DHCP-Relay-сервера можно указать в пуле DHCP Relay. Для этого войдите в режим настройки пула DHCP при помощи команды **ip dhcp pool**, затем при помощи команды **relay source** укажите подсеть-источник (source) запросов клиента, после чего при помощи команды **relay destination** укажите адрес Relay Destination Server. В пуле можно указать несколько адресов Relay Source и Relay Destination. Если пакет соответствует какому-либо из адресов Relay Source, он будет отправлен на все адреса Relay Destination.

При получении пакета DHCP-запроса, если подсеть полученного пакета соответствует Relay Source Relay-пула, пакет будет ретранслирован на основе данного пула. Чтобы ретранслировать пакет на основе пула DHCP Relay, если пакет запроса является ретранслируемым пакетом, источником запроса должен быть GIADDR (IP-адрес шлюза) пакета. Если пакет запроса не является ретранслируемым пакетом, подсеть получающего интерфейса является источником пакета.

В пуле DHCP Relay администратор может далее использовать команды **class** и **relay target**, чтобы связать список адресов Relay Target с классом DHCP. DHCP-пакет не будет ретранслирован, если на интерфейсе, принимающем пакет, не настроен IP-адрес.

Пример

В данном примере показано, как создать пул DHCP relay под именем «pool2». В Relay-пуле подсеть 172.19.18.0/255.255.255.0 указана в качестве подсети-источника (source), а 10.2.1.10 указан в качестве адреса Relay Destination.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool2
Switch(config-dhcp-pool)#relay source 172.19.18.0 255.255.255.0
Switch(config-dhcp-pool)#relay destination 10.2.1.10
Switch(config-dhcp-pool)#
```

16.20 relay target

Данная команда используется, чтобы указать DHCP Relay Target для ретранслируемых пакетов в соответствии с шаблоном значений опции, установленной в классе. Для удаления Relay Target воспользуйтесь формой **no** этой команды.

relay target *IP-ADDRESS*
no relay target *IP-ADDRESS*

Параметры

IP-ADDRESS	Укажите IP-адрес сервера relay target для класса.

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Configuration Mode.

Использование команды

Администратор может далее использовать команды **class** и **relay target**, чтобы связать список адресов Relay Target с классом DHCP. Если запрос клиента соответствует Relay-пулу, а пул DHCP Relay настроен с классами, для ретрансляции запрос клиента должен соответствовать классу, указанному в пуле. Если пакет не соответствует ни одному из классов пула, он не будет повторно ретранслирован. Если класс соответствующего Relay-пула не определен, запрос будет ретранслирован в Relay Destination соответствующего Relay-пула. Для класса можно указать несколько команд Relay Target. Если пакет соответствует классу, он будет направлен во все Relay Targets (Destination).

Если для класса не настроена команда **relay target**, за Relay Target будет принято Relay Destination, указанное для пула. DHCP-пакет не будет ретранслирован, если на интерфейсе, принимающем пакет, не настроен IP-адрес.

Пример

В данном примере показано, как настроить DHCP Relay Target для ретрансляции пакетов, которая соответствует образцу значений опции, установленной в классе.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-A
Switch(config-dhcp-class)#option 60 hex 112233
Switch(config-dhcp-class)#option 60 hex 102030
Switch(config-dhcp-class)#exit
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#relay source 172.19.18.0 255.255.255.0
Switch(config-dhcp-pool)#class Service-A
Switch(config-dhcp-pool-class)#relay target 10.2.1.2
Switch(config-dhcp-pool-class)#
```

16.21 service dhcp

Данная команда используется для включения сервиса DHCP Relay на коммутаторе. Для отключения сервиса DHCP Relay воспользуйтесь формой **no** этой команды.

service dhcp

no service dhcp

Параметры

Нет.

По умолчанию

По умолчанию сервис отключен.

Режим ввода команды

Global Configuration Mode.

Использование команды

Команда применяется для включения/отключения DHCP-сервера и сервиса DHCP Relay на коммутаторе.

Пример

В данном примере показано, как отключить DHCP-сервер и сервис DHCP Relay.

```
Switch#configure terminal
Switch(config)#no service dhcp
Switch(config)#
```

16.22 show ip dhcp relay information trusted-sources

Данная команда используется для отображения всех интерфейсов, настроенных в качестве доверенных источников для опции DHCP Relay.

show ip dhcp relay information trusted-sources

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Команда применяется для отображения рабочих настроек функции Trust Relay Option.

Пример

В данном примере показано, как отобразить рабочие настройки Trust Relay Option, когда команда **ip dhcp relay information trust-all** отключена.

```
Switch#show ip dhcp relay information trusted-sources

List of trusted sources of relay agent information option:
vlan100             vlan200             vlan300             vlan400
vlan500

Total Entries: 5

Switch#
```

В примере ниже показано, как отобразить рабочие настройки Trust Relay Option, когда команда **ip dhcp relay information trust-all** включена.

```
Switch#show ip dhcp relay information trusted-sources

All interfaces are trusted source of relay agent information option

Switch#
```

16.23 show ip dhcp relay information option format-type

Данная команда используется для отображения настроек формата опций интерфейса.

show ip dhcp relay information option format-type [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите для отображения информации об интерфейсе.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Команда позволяет отобразить настройки формата опций интерфейса. Если параметр не указан, будет отображена информация обо всех интерфейсах.

Пример

В данном примере показано, как отобразить настройки формата опций интерфейса.

```
Switch#show ip dhcp relay information option format-type

eth1/0/1
Remote ID vendor string: string1
eth1/0/2
Circuit ID vendor string: string1
eth1/0/3
Remote ID vendor string: string3
Circuit ID vendor string: string4

Total Entries: 3

Switch#
```

16.24 show ip dhcp relay information option-insert

Данная команда используется для отображения настройки встраивания Relay Option.

show ip dhcp relay information option-insert

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду для отображения Relay Information Option и информации о настройке встраивания.

Пример

В данном примере показано, как отобразить информацию об Option 82 и информацию о настройке встраивания этой опции для всех VLAN.

```
Switch#show ip dhcp relay information option-insert

Interface     Option-Insert
------------ ----------
vlan1         Enabled
vlan2         Disabled
vlan3         Not Configured

Total Entries: 3

Switch#
```

16.25 show ip dhcp relay information policy-action

Данная команда позволяет отобразить информацию об алгоритме перенаправления Relay Option для интерфейса.

show ip dhcp relay information policy-action

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду для отображения информации об алгоритме перенаправления Relay Option.

Пример

В данном примере показано, как отобразить информацию об алгоритме перенаправления Option 82 для всех VLAN.

```
Switch# show ip dhcp relay information policy-action

Interface      Policy
-------------- ----------
vlan1          Keep
vlan2          Drop
vlan3          Replace
vlan4          Not configured

Total Entries: 4

Switch#
```

17. Команды DHCP Server Screening

17.1 based-on hardware-address

Данная команда используется для добавления записи профиля DHCP Server Screen. Чтобы удалить запись, воспользуйтесь формой **no** этой команды.

based-on hardware-address *CLIENT-HARDWARE-ADDRESS*
no based-on hardware-address *CLIENT-HARDWARE-ADDRESS*

Параметры

CLIENT-HARDWARE-ADDRESS	Укажите MAC-адрес клиента.

По умолчанию

Нет.

Режим ввода команды

DHCP Server Screen Configure Mode.

Использование команды

Будет разрешена отправка сообщения сервера с IP-адресом указанного сервера и адресом клиента в пакете. Согласно данным записям привязок, только указанным серверам разрешено назначать адреса указанным клиентам.

Пример

В данном примере показано, как настроить профиль DHCP Server Screen «campus-profile», содержащий список MAC-адресов клиентов.

```
Switch# configure terminal
Switch(config)# dhcp-server-screen profile campus-profile
Switch(config-dhcp-server-screen)# based-on hardware-address 00-08-01-02-03-04
Switch(config-dhcp-server-screen)# based-on hardware-address 00-08-01-03-00-01
Switch(config-dhcp-server-screen)#
```

17.2 clear ip dhcp snooping server-screen log

Используйте данную команду, чтобы очистить буфер журнала событий Server Screen.

clear ip dhcp snooping server-screen log

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Использование команды

Используйте данную команду, чтобы очистить буфер журнала событий Server Screen. Буфер журнала событий DHCP Server Screen хранит информацию о пакетах, которые не прошли screening. Первый пакет, который не прошел проверку, будет отправлен в модуль журнала событий и записан в буфер. Последующие пакеты из той же сессии не будут отправляться в модуль журнала событий, пока его запись в буфере не будет удалена.

Пример

В данном примере показано, как очистить журнал событий Server Screen.

```
Switch# clear ip dhcp snooping server-screen log
Switch#
```

17.3 dhcp-server-screen profile

Данная команда используется для настройки профиля Server Screen и входа в режим DHCP Server Screen Configure Mode. Используйте форму **no** для удаления профиля Server Screen.

dhcp-server-screen profile *PROFILE-NAME*
no dhcp-server-screen profile *PROFILE-NAME*

Параметры

PROFILE-NAME	Укажите имя профиля. Максимально допустимое количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы войти в режим DHCP Server Screen Configure Mode и настроить профиль Server Screen. Профиль можно использовать для настройки записи DHCP Server Screen.

Пример

В данном примере показано, как войти в режим DHCP Server Screen Configure Mode и настроить профиль «campus».

```
Switch#configure terminal
Switch(config)#service dhcp
Switch(config)#dhcp-server-screen profile campus
Switch(config-dhcp-server-screen)#
```

17.4 ip dhcp snooping server-screen

Данная команда используется для включения DHCP Server Screening. Используйте форму **no** для отключения данной функции.

ip dhcp snooping server-screen [*SERVER-IP-ADDRESS* **profile** *PROFILE-NAME*]
no ip dhcp snooping server-screen [*SERVER-IP-ADDRESS*]

Параметры

SERVER-IP-ADDRESS	(Опционально.) Укажите IP-адрес доверенного DHCP-сервера.
profile *PROFILE-NAME*	(Опционально) Укажите профиль со списком MAC-адресов клиентов для DHCP-сервера.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Команда применима исключительно для настройки физического порта и port-channel.

Функция DHCP Server Screening используется для фильтрации пакетов DHCP-сервера на указанном интерфейсе, а также для получения доверенных пакетов из указанного источника. Данная функция позволяет защитить сеть в случае, когда пакеты DHCP-сервера отправляются вредоносным узлом.

По умолчанию функция DHCP Server Screening отключена на всех интерфейсах. При ее включении все пакеты DHCP-сервера на указанном интерфейсе будут отфильтрованы и будут переданы только пакеты от доверенного сервера.

Если запись Server Screen определена в профиле, который содержит MAC-адрес клиента, будет передано сообщение сервера с IP-адресом сервера и адресами клиентов, содержащимися в профиле.

Если запись настроена без MAC-адреса клиента, будет передано сообщение сервера с IP-адресом указанного сервера. Каждый сервер может иметь только одну соответствующую запись в таблице.

Если запись определена в профиле, но записи не существует, сообщения с IP-адресом сервера, указанным в записи, не передаются.

Пример

В данном примере показано, как настроить профиль DHCP Server Screen «campus-profile» и ассоциировать его с записью DHCP Server Screen для порта 3.

```
Switch#configure terminal
Switch(config)#dhcp-server-screen profile campus-profile
Switch(config-dhcp-server-screen)#based-on hardware-address 00-08-01-02-03-04
Switch(config-dhcp-server-screen)#based-on hardware-address 00-08-01-03-00-01
Switch(config-dhcp-server-screen)#exit
Switch(config)#interface eth1/0/3
Switch(config-if)#ip dhcp snooping server-screen 10.1.1.2 profile campus-profile
Switch(config-if)#
```

17.5 ip dhcp snooping server-screen log-buffer

Данная команда используется для настройки буфера журнала событий DHCP Server Screen. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ip dhcp snooping server-screen log-buffer entries *NUMBER*
no ip dhcp snooping server-screen log-buffer entries

Параметры

NUMBER	Укажите количество записей в буфере. Максимальное значение – 1024.

По умолчанию

Значение по умолчанию – 32.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для настройки максимального количества записей в буфере журнала событий. Буфер журнала событий DHCP Server Screen хранит информацию о пакетах, которые не прошли screening. Первый пакет, который не прошел проверку, будет отправлен в модуль журнала событий и записан в буфер. Последующие пакеты из той же сессии не будут отправлены в модуль журнала событий, пока его запись в буфере не будет удалена.

Если буфер журнала событий заполнен, а события (нарушения) продолжают поступать, пакеты будут отброшены, но события не будут отправлены в модуль системного журнала. Если пользователь задает размер буфера меньше текущего номера записи, буфер журнала будет очищен автоматически.

Пример

В данном примере показано, как изменить размер буфера на 64.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping server-screen log-buffer entries 64
Switch(config)#
```

17.6 show ip dhcp server-screen log

Данная команда используется для отображения буфера журнала событий Server Screen.

show ip dhcp server-screen log

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить содержимое буфера журнала событий DHCP Server Screen. Буфер хранит информацию о сообщениях сервера, которые не прошли screening. Фиксируется количество нарушений одного и того же типа, а также время последнего нарушения.

Пример

В данном примере показано, как отобразить буфер журнала событий DHCP Server Screen.

```
Switch#show ip dhcp server-screen log

Total log buffer size: 64

VLAN          Server IP                Client MAC               Occurrence
---------- -------------------- -------------------- ----------------------------

100            10.20.1.1               00-20-30-40-50-60       06:30:37, 2013-02-07
100            10.58.2.30              10-22-33-44-50-60       06:31:42, 2013-02-07

Total Entries: 2

Switch#
```

17.7 snmp-server enable traps dhcp-server-screen

Данная команда используется для включения отправки SNMP-уведомлений об атаках, поступающих от ложного DHCP-сервера. Используйте форму **no** для отключения отправки SNMP-уведомлений.

snmp-server enable traps dhcp-server-screen

no snmp-server enable traps dhcp-server-screen

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Если после запуска функции DHCP Server Screening коммутатор получил от ложного DHCP-сервера атакующий пакет, данное событие будет занесено в журнал. Используйте данную команду, чтобы включить/отключить отправку SNMP-уведомлений о подобных событиях.

Пример

В данном примере показано, как включить отправку trap-сообщений для DHCP Server Screening.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps dhcp-server-screen
Switch(config)#
```

18. Команды DHCP Snooping

18.1 ip dhcp snooping

Данная команда используется для глобального включения DHCP Snooping. Используйте форму **no**, чтобы отключить DHCP Snooping.

ip dhcp snooping

no ip dhcp snooping

Параметры

Нет.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Функция DHCP Snooping отслеживает пакеты DHCP, поступающие на недоверенный интерфейс в VLAN. С помощью данной функции DHCP-пакеты с недоверенного интерфейса могут получить статус проверенных и будет создана таблица привязки DHCP Snooping в VLAN. Таблица привязки содержит информацию о привязке IP и MAC, которая позже дополнительно может использоваться IP Source Guard и Dynamic ARP Inspection.

Пример

В данном примере показано, как включить DHCP Snooping.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping
Switch(config)#
```

18.2 ip dhcp snooping information option allow-untrusted

Данная команда используется для глобального доступа DHCP-пакетов с Relay Option 82 к недоверенным интерфейсам. Используйте форму **no**, чтобы запретить пакеты с Relay Option 82.

ip dhcp snooping information option allow-untrusted

no ip dhcp snooping information option allow-untrusted

Параметры

Нет.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Функция DHCP Snooping проверяет пакеты DHCP, когда они поступают на порт в VLAN, на которой включена функция DHCP Snooping. По умолчанию при проверке будут отброшены пакеты, если адрес шлюза не равен 0 или присутствует Option 82.
Используйте данную команду, чтобы разрешить/запретить пакетам с Relay Option 82 доступ к недоверенным интерфейсам.

Пример

В данном примере показано, как включить DHCP Snooping для Option 82, чтобы разрешить доступ к недоверенным интерфейсам.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping information option allow-untrusted
Switch(config)#
```

18.3 ip dhcp snooping database

Данная команда используется для настройки хранения записей привязки DHCP Snooping на удаленном узле. Для отключения хранения или возврата к настройкам по умолчанию используйте команду **no**.

ip dhcp snooping database {*URL* **| write-delay** *SECONDS***}**

no ip dhcp snooping database [write-delay]

Параметры

URL	Укажите URL в следующем формате: • tftp://location/filename
write-delay *SECONDS*	Укажите время ожидания перед обновлением записи при обнаружении изменений в таблице привязки. Время по умолчанию составляет 300 секунд. Диапазон значений: от 60 до 86400.

По умолчанию

По умолчанию URL-адрес агента базы данных не установлен.
Значение времени задержки для записи по умолчанию составляет 300 секунд.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для сохранения записей привязки DHCP на удаленном узле через TFTP.

Время аренды записи (Lease Time) не будет изменено, и время жизни (Live Time) продолжит отсчитываться, пока запись существует.

Пример

В данном примере показано, как настроить сохранение привязки в файл.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping database tftp: //10.0.0.2/store/dhcp-snp-bind
Switch(config)#
```

18.4 clear ip dhcp snooping database statistics

Данная команда используется для удаления статистики таблицы привязки DHCP.

clear ip dhcp snooping database statistics

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда позволяет удалить статистику таблицы привязки DHCP.

Пример

В данном примере показано, как удалить статистику таблицы привязки DHCP Snooping.

```
Switch#clear ip dhcp snooping database statistics
Switch#
```

18.5 clear ip dhcp snooping binding

Данная команда используется для удаления привязки DHCP.

clear ip dhcp snooping binding [*MAC-ADDRESS***] [***IP-ADDRESS***] [vlan** *VLAN-ID***] [interface** *INTERFACE-ID***]**

Параметры

MAC-ADDRESS	(Опционально.) Укажите MAC-адрес, который необходимо удалить.

IP-ADDRESS	(Опционально.) Укажите IP-адрес, который необходимо удалить.
vlan *VLAN-ID*	(Опционально.) Укажите VLAN ID, который необходимо удалить.
interface *INTERFACE-ID*	(Опционально.) Укажите интерфейс, который необходимо удалить.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда позволяет удалить запись привязки DHCP, включая заданные вручную записи привязки.

Пример

В данном примере показано, как удалить все записи привязки DHCP Snooping.

```
Switch#clear ip dhcp snooping binding
Switch#
```

18.6 renew ip dhcp snooping database

Данная команда используется для обновления таблицы привязки DHCP.

renew ip dhcp snooping database *URL*

Параметры

URL	Укажите URL в следующем формате: • tftp://location/filename

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для обновления таблицы привязки DHCP с URL-адреса и добавления записей в таблицу привязки DHCP Snooping.

Пример

В данном примере показано, как обновить таблицу привязки DHCP Snooping.

```
Switch#renew ip dhcp snooping database tftp: //10.0.0.2/store/dhcp-snp-bind
Switch#
```

18.7 ip dhcp snooping binding

Данная команда используется для настройки привязки DHCP Snooping вручную.

ip dhcp snooping binding *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **expiry** *SECONDS*

Параметры

MAC-ADDRESS	Укажите MAC-адрес записи, которую необходимо добавить или удалить.
vlan *VLAN-ID*	Укажите VLAN ID записи, которую необходимо добавить или удалить.
IP-ADDRESS	Укажите IP-адрес записи, которую необходимо добавить или удалить.
INTERFACE-ID	Укажите интерфейс, на котором необходимо добавить или удалить запись привязки.
SECONDS	Укажите интервал, после которого привязки не будут действительны. Доступен диапазон значений от 60 до 4294967295 секунд.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Даннакая команда применима исключительно для настройки интерфейсов физических портов и port-channel.
Команда используется для создания динамической записи DHCP Snooping.

Пример

В данном примере показано, как настроить запись DHCP Snooping с IP-адресом 10.1.1.1 и MAC-адресом 00-01-02-03-04-05 для VLAN 2 и интерфейса Ethernet 1/0/10 с expiry time 100 секунд.

```
Switch#ip dhcp snooping binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface eth1/0/10 expiry
100
Switch#
```

18.8 ip dhcp snooping trust

Данная команда используется для настройки порта в качестве доверенного интерфейса для DHCP Snooping. При использовании формы **no** команда вернется к значениям по умолчанию.

ip dhcp snooping trust

no ip dhcp snooping trust

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физических портов и port-channel.

Порты, подключенные к DHCP-серверу или к другим коммутаторам, должны быть настроены как доверенные интерфейсы. Порты, подключенные к DHCP-клиентам, должны быть настроены как недоверенные интерфейсы. DHCP Snooping работает в качестве межсетевого экрана между недоверенными интерфейсами и DHCP-серверами.

Если порт настроен как недоверенный интерфейс, сообщение DHCP придет на порт в ту VLAN, в которой включен DHCP Snooping. Коммутатор перенаправит пакеты DHCP, если только не будет соблюдаться любое из следующих условий (в таком случае пакеты будут отбрасываться):

- Порт коммутатора получает пакет (например, пакет DHCPOFFER, DHCPACK, DHCPNAK) от DHCP-сервера за пределами межсетевого экрана.
- Если включена команда **ip dhcp snooping verify mac-address**, чтобы пройти проверку, MAC-адрес источника в заголовке Ethernet должен быть таким же, как и аппаратный адрес DHCP-клиента.
- Недоверенный интерфейс получает DHCP-пакет, включающий в себя IP-адрес агента ретрансляции (Relay Agent), отличный от 0.0.0.0, или Relay Agent перенаправляет пакет, включающий в себя Option 82 на недоверенный интерфейс.
- Маршрутизатор получает сообщение DHCPRELEASE или DHCPDECLINE от недоверенного узла с записью в таблице привязки DHCP Snooping, и информация об интерфейсе в таблице привязки не соответствует интерфейсу, на котором было получено сообщение.

В дополнение к процессу проверки DHCP Snooping также создает запись в таблице привязки на основе IP-адреса, назначенного клиенту сервером. Запись привязки содержит информацию, включающую MAC-адрес, IP-адрес, VLAN ID и идентификатор порта (port ID), к которому подключен клиент, а также время истечения срока аренды (lease time).

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/3 в качестве доверенного для DHCP Snooping.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#
```

18.9 ip dhcp snooping limit entries

Данная команда используется для настройки количества записей привязки DHCP Snooping, которые может изучить интерфейс. При использовании формы **no** команда сбросит значение ограничения записей DHCP.

ip dhcp snooping limit entries *NUMBER*

no ip dhcp snooping limit entries

Параметры

NUMBER	Укажите ограничение количества привязок DHCP Snooping на порт. Диапазон значений: от 0 до 1024.

По умолчанию

По умолчанию ограничений на количество записей нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физических портов и port-channel. Команда действует только на недоверенных интерфейсах. Система перестанет изучать привязки, связанные с портом, если превышено максимальное значение.

Пример

В данном примере показано, как настроить ограничение количества привязок (используется значение 100) на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip dhcp snooping limit entries 100
Switch(config-if)#
```

18.10 ip dhcp snooping limit rate

Данная команда используется для настройки количества DHCP-сообщений, которые интерфейс сможет получать за секунду. При использовании формы **no** команда сбросит значение ограничения сообщений DHCP.

ip dhcp snooping limit rate *VALUE*

no ip dhcp snooping limit rate

Параметры

VALUE	Укажите количество DHCP-сообщений, которое может быть обработано за секунду. Доступные значения: от 1 до 300.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

При превышении указанного количества DHCP-пакетов за секунду порт будет отключен из-за ошибки.

Пример

В данном примере показано, как настроить количество сообщений DHCP, которое коммутатор сможет получить на интерфейсе Ethernet 1/0/3 за одну секунду.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ip dhcp snooping limit rate 100
Switch(config-if)#
```

18.11 ip dhcp snooping station-move deny

Данная команда используется для отключения состояния DHCP Snooping Station Move. При использовании формы **no** команда включит состояние DHCP Snooping Roaming.

ip dhcp snooping station-move deny

no ip dhcp snooping station-move deny

Параметры

Нет.

По умолчанию

По умолчанию опция включена.

Режим ввода команды

Global Configuration Mode.

Использование команды

При включении DHCP Snooping Station Move динамическая запись привязки DHCP Snooping с теми же VLAN ID и MAC-адресом на определенном порту может переместиться на другой порт, если обнаружится, что новому процессу DHCP принадлежит тот же VLAN ID и MAC-адрес.

Пример

В данном примере показано, как отключить состояние Roaming.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 10
Switch(config)#ip dhcp snooping station-move deny
Switch(config)#
```

18.12 ip dhcp snooping verify mac-address

Данная команда используется для включения проверки совпадения MAC-адреса источника в DHCP-пакете и аппаратного адреса клиента. При использовании формы **no** команда отключит проверку MAC-адреса.

ip dhcp snooping verify mac-address
no ip dhcp snooping verify mac-address

Параметры

Нет.

По умолчанию

По умолчанию опция включена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Функция DHCP Snooping проверяет DHCP-пакеты, присылаемые на порт в VLAN, на которой включена функция DHCP Snooping. По умолчанию DHCP Snooping проверяет, совпадает ли MAC-адрес источника в пакете с аппаратным адресом DHCP-клиента.

Пример

В данном примере показано, как включить проверку на соответствие MAC-адреса источника в DHCP-пакете аппаратному адресу клиента.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping verify mac-address
Switch(config)#
```

18.13 ip dhcp snooping vlan

Данная команда используется для включения DHCP Snooping в VLAN или группе VLAN. При использовании формы **no** команда отключит DHCP Snooping в VLAN или группе VLAN.

ip dhcp snooping vlan *VLAN-ID* **[, | -]**
no ip dhcp snooping vlan *VLAN-ID* **[, | -]**

Параметры

VLAN-ID	Укажите VLAN, которую необходимо использовать.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию функция DHCP Snooping включена во всех VLAN.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду для включения DHCP Snooping для VLAN. Функция DHCP Snooping отслеживает пакеты DHCP, поступающие на недоверенный интерфейс в VLAN. С помощью данной функции DHCP-пакеты с недоверенного интерфейса могут получить статус проверенных и будет создана таблица привязки DHCP Snooping в VLAN. Таблица привязки содержит информацию о привязке IP и MAC, которая позже дополнительно может использоваться IP Source Guard и Dynamic ARP Inspection.

Пример

В данном примере показано, как включить DHCP Snooping в VLAN 10.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping vlan 10
Switch(config)#
```

В следующем примере показано, как отключить DHCP Snooping в нескольких VLAN.

```
Switch#configure terminal
Switch(config)# no ip dhcp snooping vlan 10,15-18
Switch(config)#
```

18.14 show ip dhcp snooping

Данная команда используется для отображения настроек DHCP Snooping.

show ip dhcp snooping

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для отображения настроек DHCP Snooping.

Пример

В данном примере показано, как отобразить конфигурацию DHCP Snooping.

```
Switch# show ip dhcp snooping

DHCP Snooping is disabled
DHCP Snooping is enabled on VLANs:
     1-4094
Verification of MAC address is enabled
Station move is permitted.
Information option is not allowed on un-trusted interface

Interface      Trusted   Rate Limit   Entry Limit
-------------- --------- ------------ ------------
eth1/0/1       no        10           no_limit
eth1/0/2       no        no_limit     no_limit
eth1/0/3       no        no_limit     no_limit
eth1/0/4       no        no_limit     no_limit
eth1/0/5       no        no_limit     no_limit
eth1/0/6       no        no_limit     no_limit
eth1/0/7       no        no_limit     no_limit
eth1/0/8       no        50           20
eth1/0/9       yes       no_limit     no_limit
eth1/0/10      no        no_limit     no_limit
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

18.15 show ip dhcp snooping binding

Данная команда используется для отображения записей привязки DHCP Snooping.

show ip dhcp snooping binding [*IP-ADDRESS***] [***MAC-ADDRESS***] [vlan** *VLAN-ID***] [interface** *INTERFACE-ID* **[[, | -]]]**

Параметры

IP-ADDRESS	(Опционально.) Укажите, если необходимо отображать привязки на основе IP-адреса.
MAC-ADDRESS	(Опционально.) Укажите, если необходимо отображать привязки на основе MAC-адреса.

vlan *VLAN-ID*	(Опционально.) Укажите, если необходимо отображать привязки на основе VLAN.
interface	(Опционально.) Укажите, если необходимо отображать привязки на основе ID порта (port ID).
INTERFACE-ID	(Опционально.) Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для отображения записей привязки DHCP Snooping.

Пример

В данном примере показано, как отобразить все записи привязки DHCP Snooping.

```
Switch#show ip dhcp snooping binding

MAC Address       IP Address      Lease(seconds) Type          VLAN Interface
----------------- --------------- -------------- ------------- ---- --------------
00-01-02-03-04-05 10.1.1.10       1500           dhcp-snooping 100  eth1/0/5
00-01-02-00-00-05 10.1.1.11       1495           dhcp-snooping 100  eth1/0/5

Total Entries: 2

Switch#
```

В данном примере показано, как отобразить запись привязки DHCP Snooping по IP 10.1.1.10.

```
Switch# show ip dhcp snooping binding 10.1.1.10

MAC Address       IP Address      Lease(seconds) Type        VLAN Interface
----------------- --------------- -------------- ------------- ---- -------------
00-01-02-03-04-05 10.1.1.10       1500         dhcp-snooping 100  eth1/0/5

Total Entries: 1

Switch#
```

В следующем примере показано, как отобразить запись привязки DHCP Snooping для IP 10.1.1.10 и MAC 00-01-02-00-00-05.

```
Switch# show ip dhcp snooping binding 10.1.1.10 00-01-02-03-04-05

MAC Address       IP Address      Lease(seconds) Type        VLAN Interface
----------------- --------------- -------------- ----------- ---- -------------
00-01-02-03-04-05 10.1.1.10       1495           dhcp-snooping 100  eth1/0/5

Total Entries: 1

Switch#
```

В следующем примере показано, как отобразить запись привязки DHCP Snooping для IP 10.1.1.10 и MAC 00-01-02-03-04-05 в VLAN 100.

```
Switch# show ip dhcp snooping binding 10.1.1.10 00-01-02-03-04-05 vlan 100

MAC Address       IP Address      Lease(seconds) Type        VLAN Interface
----------------- --------------- -------------- ----------- ---- -------------
00-01-02-03-04-05 10.1.1.10       1495           dhcp-snooping 100  eth1/0/5

Total Entries: 1

Switch#
```

В примере ниже показано, как отобразить записи привязки DHCP Snooping в VLAN 100.

```
Switch#show ip dhcp snooping binding vlan 100

MAC Address       IP Address      Lease(seconds) Type          VLAN Interface
----------------- --------------- -------------- ------------ ---- --------------
00-01-02-03-04-05 10.1.1.10       1500           dhcp-snooping 100  eth1/0/5
00-01-02-00-00-05 10.1.1.11       1495           dhcp-snooping 100  eth1/0/5

Total Entries: 2

Switch#
```

В примере ниже показано, как отобразить записи привязки DHCP Snooping на интерфейсе Ethernet 1/0/5.

```
Switch#show ip dhcp snooping binding interface eth1/0/5

MAC Address       IP Address      Lease(seconds) Type          VLAN Interface
----------------- --------------- -------------- ------------ ---- --------------
00-01-02-03-04-05 10.1.1.10       1500           dhcp-snooping 100  eth1/0/5
00-01-02-00-00-05 10.1.1.11       495            dhcp-snooping 100  eth1/0/5

Total Entries: 2

Switch#
```

Отображаемые параметры

MAC Address	Аппаратный MAC-адрес клиента.

IP Address	IP-адрес клиента, назначенный DHCP-сервером.
Lease (seconds)	Время аренды IP-адреса.
Type	Тип привязки, настроенный через интерфейс командной строки или изученный динамически.
VLAN	VLAN ID.
Interface	Интерфейс, к которому подключен DHCP-клиент.

18.16 show ip dhcp snooping database

Данная команда используется для отображения статистики таблицы привязок DHCP Snooping.

show ip dhcp snooping database

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для отображения статистики таблицы привязок DHCP Snooping.

Пример

В данном примере показано, как отобразить статистику таблицы привязок DHCP Snooping.

```
Switch#show ip dhcp snooping database

URL:  tftp:  //10.0.0.2/store/dhcp-snp-bind
Write Delay Time:  300 seconds

Last ignored bindings counters:
Binding collisions :   0         Expired    lease  :   0
Invalid interfaces :   0         Unsupported vlans :   0
Parse failures     :   0         Checksum errors   :   0

Switch#
```

Отображаемые параметры

Binding Collisions	Количество записей, создавших коллизии с существующими записями в таблице привязок DHCP Snooping.

Expired leases	Количество записей с истекшим сроком аренды в таблице привязок DHCP Snooping.
Invalid interfaces	Количество интерфейсов, получивших сообщение DHCP, для которых не выполняется DHCP Snooping.
Parse failures	Количество недопустимых пакетов DHCP.
Checksum errors	Количество подсчитанных значений контрольной суммы, отличных от сохраненного значения контрольной суммы.
Unsupported vlans	Количество записей, для которых VLAN отключена.

18.17 clear ip dhcp snooping server-screen log

Используйте данную команду, чтобы очистить буфер журнала событий Server Screen.

clear ip dhcp snooping server-screen log

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы очистить буфер журнала событий Server Screen. Буфер журнала событий DHCP Server Screen хранит информацию о пакетах, которые не прошли screening. Первый пакет, который не прошел проверку, будет отправлен в модуль журнала событий и записан в буфер журнала событий Server Screen. Последующие пакеты из той же сессии не будут отправлены в модуль журнала событий, если его запись в буфере журнала событий не будет удалена.

Пример

В данном примере показано, как очистить журнал событий Server Screen.

```
Switch# clear ip dhcp snooping server-screen log
Switch#
```

18.18 dhcp-server-screen profile

Данная команда используется для настройки профиля Server Screen и входа в режим Server Screen Configure Mode. Используйте форму **no** для удаления профиля Server Screen.

dhcp-server-screen profile *PROFILE-NAME*
no dhcp-server-screen profile *PROFILE-NAME*

Параметры

PROFILE-NAME	Укажите имя профиля. Максимально допустимое количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы войти в режим DHCP Server Screen Configure Mode и настроить профиль Server Screen. Профиль можно использовать для настройки записи DHCP Server Screen.

Пример

В данном примере показано, как войти в режим DHCP Server Screen Configure Mode и настроить профиль «campus».

```
Switch# configure terminal
Switch(config)# service dhcp
Switch(config)# dhcp-server-screen profile campus
Switch(config-dhcp-server-screen)#
```

18.19 ip dhcp snooping server-screen

Данная команда используется для включения DHCP Server Screening. Используйте форму **no** для отключения данной функции.

ip dhcp snooping server-screen [*SERVER-IP-ADDRESS* **profile** *PROFILE-NAME***]**
no ip dhcp snooping server-screen [*SERVER-IP-ADDRESS***]**

Параметры

SERVER-IP-ADDRESS	(Опционально.) Укажите IP-адрес доверенного DHCP-сервера.
profile *PROFILE-NAME*	(Опционально) Укажите профиль со списком MAC-адресов клиентов для DHCP-сервера.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Функция DHCP Server Screening используется для фильтрации пакетов DHCP-сервера на указанном интерфейсе, а также для получения доверенных пакетов из указанного источника. Данная функция позволяет защитить сеть в случае, когда пакеты DHCP-сервера отправляются вредоносным узлом.
Если IP-адрес сервера не указан, на интерфейсе будет включен/отключен DHCP Server Screen. По умолчанию функция DHCP Server Screening отключена на всех интерфейсах. При ее включении все пакеты DHCP-сервера на указанном интерфейсе будут отфильтрованы и будут переданы только пакеты от доверенного сервера.
Если запись Server Screen определена в профиле, который содержит MAC-адрес клиента, будет передано сообщение сервера с IP-адресом сервера и адресами клиентов, содержащимися в профиле.
Если запись настроена без MAC-адреса клиента, будет передано сообщение сервера с IP-адресом указанного сервера. Каждый сервер может иметь только одну соответствующую запись в таблице.
Если запись определена в профиле, но записи не существует, сообщения с IP-адресом сервера, указанным в записи, не передаются.

Пример

В данном примере показано, как настроить профиль DHCP Server Screen «campus-profile» и ассоциировать его с записью DHCP Server Screen для порта 3.

```
Switch#configure terminal
Switch(config)#dhcp-server-screen profile campus-profile
Switch(config-dhcp-server-screen)#based-on hardware-address 00-08-01-02-03-04
Switch(config-dhcp-server-screen)#based-on hardware-address 00-08-01-03-00-01
Switch(config-dhcp-server-screen)#exit
Switch(config)#interface eth1/0/3
Switch(config-if)#ip dhcp snooping server-screen 10.1.1.2 profile campus-profile
Switch(config-if)#
```

18.20 ip dhcp snooping server-screen log-buffer

Данная команда используется для настройки буфера журнала событий DHCP Server Screen. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ip dhcp snooping server-screen log-buffer entries *NUMBER*
no ip dhcp snooping server-screen log-buffer entries

Параметры

NUMBER	Укажите количество записей в буфере. Максимальное значение – 1024.

По умолчанию

Значение по умолчанию – 32.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для настройки максимального количества записей в буфере журнала событий. Буфер журнала событий DHCP Server Screen хранит информацию о пакетах, которые не прошли screening. Первый пакет, который не прошел проверку, будет отправлен в модуль журнала событий и записан в буфер. Последующие пакеты из той же сессии не будут отправлены в модуль журнала событий, пока его запись в буфере не будет удалена.
Если буфер журнала событий заполнен, а события (нарушения) продолжают поступать, пакеты будут отброшены, но события не будут отправлены в модуль системного журнала. Если пользователь задает размер буфера меньше текущего номера записи, буфер журнала будет очищен автоматически.

Пример

В данном примере показано, как изменить размер буфера на 64.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping server-screen log-buffer entries 64
Switch(config)#
```

18.21 show ip dhcp server-screen log

Данная команда используется для отображения буфера журнала событий Server Screen.

show ip dhcp server-screen log

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить содержимое буфера журнала событий DHCP Server Screen. Буфер хранит информацию о сообщениях сервера, которые не прошли screening. Фиксируется количество нарушений одного и того же типа, а также время последнего нарушения.

Пример

В данном примере показано, как отобразить буфер журнала событий DHCP Server Screen.

```
Switch# show ip dhcp server-screen log
Total log buffer size: 64

VLAN   Server IP       Client MAC        Occurrence
------ -------------- ----------------- ----------------------
100    10.20.1.1       00-20-30-40-50-60 06:30:37, 2014-03-10
100    10.58.2.30      10-22-33-44-50-60 06:31:42, 2014-03-10

Total Entries: 2

Switch#
```

19. Команды DHCPv6 Client

19.1 clear ipv6 dhcp client

Данная команда используется для перезапуска клиента DHCPv6 на интерфейсе.

clear ipv6 dhcp client *INTERFACE-ID*

Параметры

INTERFACE-ID	Укажите интерфейс VLAN, на котором необходимо перезапустить клиент DHCPv6.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов VLAN.
Команда используется для перезапуска клиента DHCPv6 на указанном интерфейсе.

Пример

В данном примере показано, как перезапустить клиент DHCPv6 на интерфейсе VLAN 1.

```
Switch#clear ipv6 dhcp client vlan1
Switch#
```

19.2 show ipv6 dhcp

Данная команда используется для отображения настроек DHCPv6 на интерфейсе.

show ipv6 dhcp [interface [*INTERFACE-ID***]]**

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейс VLAN, для которого необходимо отобразить настройки DHCPv6.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить DHCPv6 DUID устройства, или используйте команду **show ipv6 dhcp interface**, чтобы отобразить настройки DHCPv6 на интерфейсах. Если ID интерфейса не указан, будут отображены все интерфейсы с функцией DHCPv6.

Пример

В данном примере показано, как отобразить DHCPv6 DUID для устройства.

```
Switch#show ipv6 dhcp

This device's DUID is 00030006f07d68121001

Switch#
```

В следующем примере показано, как отобразить настройки DHCPv6 для интерфейса VLAN 1. При этом функция DHCPv6 на VLAN1 отключена.

```
Switch#show ipv6 dhcp interface vlan1

vlan1 is not in DHCPv6 mode.

Switch#
```

В примере ниже показано, как отобразить настройки DHCPv6 для всех VLAN. Отображаются только те VLAN, на которых включена функция DHCPv6.

```
Switch#show ipv6 dhcp interface

vlan1 is in client mode
  State is OPEN
  List of known servers:
    Reachable via address: FE80::200:11FF:FE22:3344
    Configuration parameters:
        IA PD: IA ID 1, T1 40, T2 64
          Prefix: 2000::/48
                preferred lifetime 80, valid lifetime 100
  Prefix name: yy
  Rapid-Commit: disabled

Switch#
```

20. Команды DHCPv6 Guard

20.1 ipv6 dhcp guard policy

Данная команда используется для создания или изменения политики DHCPv6 Guard. Команда позволяет войти в режим DHCPv6 Guard Configuration Mode. Для удаления политики DHCPv6 Guard воспользуйтесь формой **no** этой команды.

ipv6 dhcp guard policy *POLICY-NAME*
no ipv6 dhcp guard policy *POLICY-NAME*

Параметры

POLICY-NAME	Укажите имя политики DHCPv6 Guard.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для создания или изменения политики DHCPv6 Guard. Команда позволяет войти в режим DHCPv6 Guard Configuration Mode. Политики DHCPv6 Guard могут использоваться для блокировки ответов DHCPv6 Reply и сообщений, приходящих с неавторизованного сервера. Сообщения клиента не блокируются.

После создания политики DHCPv6 Guard используйте команду **ipv6 dhcp guard attach-policy** для применения политики на определенном интерфейсе.

Пример

В данном примере показано, как создать политику DHCPv6 Guard.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp guard policy policy1
Switch(config-dhcp-guard)#
```

20.2 device-role

Данная команда используется для указания роли подключенного устройства. При использовании формы **no** данная команда вернется к настройкам по умолчанию.

device-role {client | server}
no device-role

Параметры

client	Укажите, чтобы настроить подключенное устройство в качестве клиента DHCPv6. Все сообщения сервера DHCPv6 на этом порту будут отбрасываться.
server	Укажите, чтобы настроить подключенное устройство в качестве сервера DHCPv6. Все сообщения сервера DHCPv6 на этом порту будут приниматься.

По умолчанию

По умолчанию настроена опция **client**.

Режим ввода команды

DHCPv6 Guard Policy Configuration Mode.

Использование команды

Данная команда используется для указания роли подключенного устройства. По умолчанию устройство выполняет роль клиента, и все сообщения сервера DHCPv6, приходящие на порт, будут отбрасываться. Если настроить устройство в качестве сервера, сообщения сервера DHCPv6 будут разрешены на данном порту.

Пример

В данном примере показано, как создать политику DHCPv6 Guard и настроить устройство в качестве сервера.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp guard policy policy1
Switch(config-dhcp-guard)# device-role server
Switch(config-dhcp-guard)#
```

20.3 match ipv6 access-list

Данная команда используется для проверки IPv6-адреса источника в сообщениях сервера. При использовании формы **no** данная команда отключит проверку.

match ipv6 access-list *IPV6-ACCESS-LIST-NAME*
no match ipv6 access-list

Параметры

IPV6-ACCESS-LIST-NAME	Укажите список доступа IPv6, с которым необходимо сверяться.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

DHCPv6 Guard Policy Configuration Mode.

Использование команды

Данная команда используется для фильтрации сообщений сервера DHCPv6 на основе IP-адреса источника. Если не настроена команда **match ipv6 access-list,** все сообщения сервера пропускаются. Список доступа настраивается с помощью команды **ipv6 access-list**.

Пример

В данном примере показано, как создать политику DHCPv6 Guard и настроить проверку соответствия адресов IPv6 со списком доступа list1.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp guard policy dhcp_filter1
Switch(config-dhcp-guard)#match ipv6 access-list list1
Switch(config-dhcp-guard)#
```

20.4 ipv6 dhcp guard attach-policy

Данная команда используется для применения политики DHCPv6 Guard на определенном интерфейсе. Для удаления привязки воспользуйтесь формой **no** этой команды.

ipv6 dhcp guard attach-policy [*POLICY-NAME***]**

no ipv6 dhcp guard attach-policy

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики DHCPv6 Guard.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда используется для применения политики DHCPv6 Guard на интерфейсе. Политики DHCPv6 Guard используются для блокировки DHCPv6-сообщений сервера или фильтрации сообщений сервера на основе IP-адреса источника. Если имя политики не указано, то политика по умолчанию настроит устройство в качестве клиента.

Пример

В данном примере показано, как применить политику DHCPv6 Guard «pol1» для интерфейса Ethernet 1/0/3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ipv6 dhcp guard attach-policy pol1
Switch(config-if)#
```

20.5 show ipv6 dhcp guard policy

Данная команда позволяет отобразить информацию о DHCPv6 Guard.

show ipv6 dhcp guard policy [*POLICY-NAME***]**

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики DHCPv6 Guard.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если имя политики не указано, будет отображаться информация для всех политик.

Пример

В данном примере показано, как отобразить информацию для всех политик.

```
Switch#show ipv6 dhcp guard policy

DHCP guard policy: default
   Device Role: DHCP client
   Target: eth1/0/3

DHCP guard policy: test1
   Device Role: DHCP server
   Source Address Match Access List: acl1
   Target: eth1/0/1

Switch#
```

Отображаемые параметры

Device Role	Роль устройства: клиент или сервер.
Target	Название интерфейса.
Source Address Match Access List	Список доступа IPv6 определенной политики.

21. Команды DHCPv6 Relay

21.1 ipv6 dhcp relay destination

Данная команда используется для того, чтобы включить DHCP для IPv6 Relay Service на интерфейсе и указать адрес назначения (destination), на который передаются сообщения клиентов. Для удаления Relay Destination воспользуйтесь формой **no** этой команды.

ipv6 dhcp relay destination *IPV6-ADDRESS* **[***INTERFACE-ID***]**
no ipv6 dhcp relay destination *IPV6-ADDRESS* **[***INTERFACE-ID***]**

Параметры

IPV6-ADDRESS	Укажите адрес DHCPv6 Relay Destination.
INTERFACE-ID	(Опционально.) Укажите выходной интерфейс для Relay Destination.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить или удалить адрес Relay Destination на интерфейсе. При удалении всех адресов Relay Destination эта функция будет отключена.
Входящие сообщения DHCPv6, поступающие от клиента, могут быть заранее ретранслированы при помощи Relay Agent. Адрес назначения, который необходимо ретранслировать, может принадлежать DHCPv6-серверу или другому DHCPv6 Relay Agent.
В качестве адреса назначения может быть использован индивидуальный или групповой адрес, оба могут быть как Link Scoped, так и Global Scoped. Для адресов Link Scoped необходимо указать интерфейс, в котором расположен адрес назначения. Для адресов Global Scoped можно указать выходной интерфейс (опционально). Если выходной интерфейс не указан, он определяется при помощи таблицы маршрутизации.
Для одного интерфейса можно указать несколько адресов Relay Destination. Если сообщение DHCPv6 ретранслируется на групповой адрес, для поля hop limit в заголовке пакета IPv6 будет установлено значение 32.

Пример

В данном примере показано, как сконфигурировать адрес Relay Destination на VLAN 1 и VLAN 2.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 vlan1
Switch(config-if)#ipv6 dhcp relay destination FE80::22:33 vlan2
Switch(config-if)#
```

21.2 ipv6 dhcp relay remote-id format

Данная команда используется для настройки sub-опции Remote ID. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 dhcp relay remote-id format {default | cid-with-user-define | user-define | expert-udf [standalone_unit_format {0 | 1}]}

no ipv6 dhcp relay remote-id format

Параметры

default — В качестве Remote ID используется системный MAC-адрес коммутатора. Формат Remote ID представлен ниже:

F01	F02	F03	F04	F05
Sub Type	VLAN ID	Module ID	Port ID	MAC Address
1 byte	2 bytes	1 byte	1 byte	6 bytes

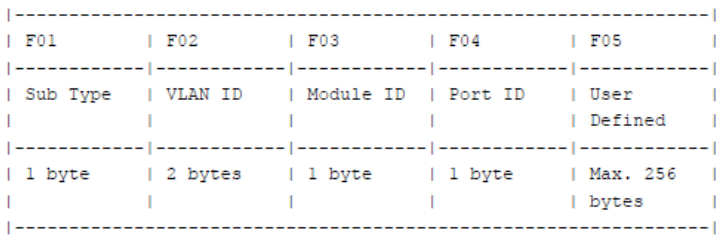
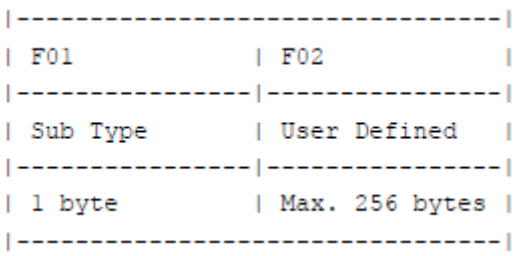
F01. *Тип sub-опции:* число 1 свидетельствует о данном типе Remote ID.

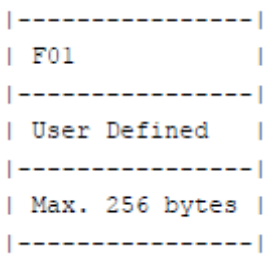
F02. *VLAN ID:* входящий VLAN ID в пакете DHCP Client.

F03. *ID модуля:* ID модуля для автономных коммутаторов – 0.

F04. *ID порта*: номер входящего порта в пакете DHCP Client. Номера портов начинаются с 1.

F05. *MAC-адрес*: системный MAC-адрес коммутатора.

cid-with-user-define	В качестве Remote ID используется CID со строкой, заданной пользователем. Формат Remote ID представлен ниже:  **F01.** *Тип sub-опции:* число 2 свидетельствует о данном типе Remote ID. **F02.** *VLAN ID:* входящий VLAN ID в пакете DHCP Client. **F03.** *ID модуля:* ID модуля для автономных коммутаторов – 0. **F04.** *ID порта*: номер входящего порта в пакете DHCP Client. Номера портов начинаются с 1. **F05.** *Задать самостоятельно*: заданная пользователем строка, настраиваемая при помощи команды **ipv6 dhcp relay remote-id udf**. По умолчанию данное поле не заполнено.
user-define	Remote ID задается самостоятельно. Формат Remote ID представлен ниже:  **F01.** *Тип sub-опции:* число 3 свидетельствует о данном типе Remote ID. **F02.** *Задать самостоятельно:* заданная пользователем строка, настраиваемая при помощи команды **ipv6 dhcp relay remote-id udf**.

expert-udf	Remote ID задается пользователем самостоятельно в виде произвольной строки. Формат Remote ID представлен ниже:  **F01.** *Задать самостоятельно:* произвольная заданная пользователем строка, настраиваемая при помощи команд **ipv6 dhcp relay remote-id format-type**, **ipv6 dhcp relay remote-id profile** и **format string**. По умолчанию данное поле не заполнено.
standalone_unit_format	Укажите Unit ID для автономного коммутатора. Значение по умолчанию – 0. Правила синтаксиса определяются командой **format string**.

По умолчанию

Формат DHCPv6 Relay Remote ID по умолчанию – **default**.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить sub-опцию Remote ID.

Пример

В данном примере показано, как настроить sub-опцию Remote ID «cid-with-user-define».

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay remote-id format cid-with-user-define
Switch(config)#
```

21.3 ipv6 dhcp relay remote-id option

Данная команда используется для того, чтобы включить встраивание Relay Agent Remote ID Option 37 в ретранслируемых пакетах запроса DHCP IPv6. Для отключения данной функции воспользуйтесь формой **no** этой команды.

ipv6 dhcp relay remote-id option

no ipv6 dhcp relay remote-id option

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы включить встраивание функции DHCPv6 Relay Agent Remote ID Option.

Пример

В данном примере показано, как включить встраивание DHCPv6 Relay Agent Remote ID Option.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay remote-id option
Switch(config)#
```

21.4 ipv6 dhcp relay remote-id policy

Данная команда используется для настройки политики перенаправления Option 37 для DHCPv6 Relay Agent. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 dhcp relay remote-id policy {drop | keep}
no ipv6 dhcp relay remote-id policy

Параметры

drop	Укажите, чтобы отбросить пакет, в котором уже есть Relay Agent Remote ID Option 37.
keep	Укажите, чтобы ретранслировать пакет запроса DHCPv6, в котором уже есть опция Remote ID, на сервер DHCPv6 в неизменном виде.

По умолчанию

Параметр по умолчанию – **keep**.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить глобальную политику для пакетов, в которых уже есть Option 37. При выборе политики **drop** полученный от клиента пакет, в котором присутствует опция Remote ID, будет отброшен. При выборе политики **keep** коммутатор не будет проверять, присутствует ли в полученном пакете опция Remote ID.

Пример

В данном примере показано, как настроить политику DHCPv6 Relay Agent Remote ID Option так, чтобы пакет был отброшен при наличии в нем опции Remote ID.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay remote-id policy drop
Switch(config)#
```

21.5 ipv6 dhcp relay remote-id profile

Данная команда используется, чтобы создать новый профиль для DHCPv6 Relay Option 37 и войти в режим DHCPv6 Profile Configuration Mode. Для удаления профиля воспользуйтесь формой **no** этой команды.

ipv6 dhcp relay remote-id profile *NAME*
no ipv6 dhcp relay remote-id profile *NAME*

Параметры

NAME	Укажите имя профиля. Максимальное количество символов – 32. Максимальное количество записей в профиле – 6.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы создать/удалить профиль для DHCPv6 Relay Option 37, а также войти в режим DHCPv6 Profile Configuration Mode.

Пример

В данном примере показано, как создать профиль «profile1» для DHCPv6 Relay Option 37.

```
Switch#configure configure terminal
Switch(config)#ipv6 dhcp relay remote-id profile profile1
Switch(config-dhcp-profile)#
```

21.6 format string

Данная команда используется для настройки заданной пользователем строки для Option 37. Для удаления записи воспользуйтесь формой **no** этой команды.

format string *STRING*
no format string

Параметры

STRING	Введите строку для использования в Option 37. Максимально допустимое количество символов – 255. Ниже представлены правила конфигурирования данного параметра: • Параметр может содержать шестнадцатеричные значения, строку ASCII или любую комбинацию шестнадцатеричных значений и строки ASCII. Строка ASCII должна быть заключена в кавычки (" "), например: "Ethernet". Символы ASCII вне кавычек будут распознаны как шестнадцатеричные значения. • Отформатированная ключевая строка – строка, которую необходимо преобразовать до того, как она будет инкапсулирована в пакет. Отформатированная ключевая строка может содержать как строки ASCII, так и шестнадцатеричные значения, например: "%" +"$"+"1-32"+"keyword"+":": **%** – указывает на то, что строка, следующая за символом, является отформатированной ключевой строкой. **$** или **0** – (опционально) индикатор заполнения. Данная опция указывает, как заполнить отформатированную ключевую строку в соответствии с требованиями по длине строки. Значение данной опции – $ или 0. **$** означает заполнение начального пробела (0x20). **0** означает заполнение начального нуля (0). Заполнение начального нуля (**0**) – настройка по умолчанию. **1-32** – (опционально) индикатор длины. Данная опция указывает, сколько символов или байтов должна занимать преобразованная ключевая строка. Если фактическая длина преобразованной ключевой строки меньше длины, предусмотренной данной опцией, будет использован индикатор заполнения. В других случаях будет использована фактическая длина строки. **keyword** – для преобразования будет использовано ключевое слово на основе фактических системных значений. При обнаружении неизвестных или неподдерживаемых ключевых слов команда будет отклонена. Доступны следующие ключевые слова: **devtype:** модель устройства. Выводится из поля Module Name в команде **show version**. Допустимо использование только строки ASCII. **sysname:** системное имя коммутатора. Допустимо использование только строки ASCII. **ifdescr:** выводится из ifDescr (IF-MIB). Допустимо использование только строки ASCII. **portmac:** MAC-адрес порта. Могут быть использованы строка ASCII или шестнадцатеричные значения. При использовании строки ASCII MAC-адрес может быть получен при помощи специальной команды (например, **ip dhcp relay information option mac-format case**). При использовании шестнадцатеричных значений MAC-адрес будет сформирован в шестнадцатеричном виде.

sysmac: системный MAC-адрес. Могут быть использованы строка ASCII или шестнадцатеричные значения. При использовании строки ASCII MAC-адрес может быть получен при помощи команд CLI (например, **ip dhcp relay information option mac-format case**). При использовании шестнадцатеричных значений MAC-адрес будет сформирован в шестнадцатеричном виде.

module: ID модуля. Могут быть использованы строка ASCII или шестнадцатеричные значения.

port: номер локального порта. Могут быть использованы строка ASCII или шестнадцатеричные значения.

svlan: ID внешней VLAN. Могут быть использованы строка ASCII или шестнадцатеричные значения.

cvlan: ID внутренней VLAN. Могут быть использованы строка ASCII или шестнадцатеричные значения.

: - конец отформатированной ключевой строки. Если отформатированная ключевая строка является последним параметром команды, ее заключительный символ (:) может быть игнорирован. Пробел (0x20) между **%** и **:** будет игнорирован. Другие пробелы будут включены.

- Строки ASCII могут содержать любые комбинации отформатированных ключевых строк, символов 0-9, a-z, A-Z, !, @, #, $, %, ^, &, *, (,), _, +, |, -, =, \, [,], {, }, ;, :, ', ", /, ., ,, <, >, ` и пробелов. **** используется в качестве знака экранирования. Специальные символы после **** являются самостоятельными символами. Например, **%** в комбинации **\%** является самостоятельным символом, а не индикатором запуска отформатированной ключевой строки. Пробелы вне отформатированной ключевой строки также будут включены.
- Шестнадцатеричные значения могут содержать любые комбинации отформатированных ключевых строк, символов 0-9, A-F, a-f и пробелов. Отформатированные ключевые строки поддерживают только те ключевые слова, в которых используются шестнадцатеричные значения. Пробелы вне отформатированной ключевой строки включены не будут.

По умолчанию

Нет.

Режим ввода команды

DHCPv6 Profile Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить строку пользователя для Option 37.

Пример

В данном примере показано, как настроить строку пользователя для Option 37.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id profile profile1
Switch(config-dhcp-profile)#format string "%port:\:%sysname:%05svlan"
Switch(config-dhcp-profile)#
```

21.7 ipv6 dhcp relay information option mac-format case

Данная команда используется для настройки формата MAC-адреса, задаваемого пользователем в профиле DHCPv6 Option 37. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 dhcp relay information option mac-format case {lowercase | uppercase} delimiter {hyphen | colon | dot | none} number {1 | 2 | 5}

no ipv6 dhcp relay information option mac-format case

Параметры

lowercase	Укажите, чтобы использовать нижний регистр при записи MAC-адреса для задаваемого пользователем профиля Option 37: aa-bb-cc-dd-ee-ff.
uppercase	Укажите, чтобы использовать верхний регистр при записи MAC-адреса для задаваемого пользователем профиля или Option 37: AA-BB-CC-DD-EE-FF.
hyphen	Укажите, чтобы использовать «-» в качестве разделителя данных: AA-BB-CC-DD-EE-FF.
colon	Укажите, чтобы использовать «:» в качестве разделителя данных: AA:BB:CC:DD:EE:FF.
dot	Укажите, чтобы использовать «.» в качестве разделителя данных: AA.BB.CC.DD.EE.FF.
none	Укажите для ввода данных без разделителя: AABBCCDDEEFF.
number	Укажите количество разделителей: **1:** один разделитель: AABBCC.DDEEFF. **2:** два разделителя: AABB.CCDD.EEFF. **5:** множество разделителей: AA.BB.CC.DD.EE.FF. Если указан параметр **none**, параметр **number** будет недействителен.

По умолчанию

Параметр регистра MAC-адреса аутентификации по умолчанию – **uppercase**.
Параметр разделителя MAC-адреса аутентификации по умолчанию – **none**.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить формат MAC-адреса, задаваемого пользователем в профиле Option 37.

Пример

В данном примере показано, как настроить формат MAC-адреса, задаваемого пользователем в профиле Option 37.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay information option mac-format case uppercase delimiter hyphen
number 5
Switch(config)#
```

21.8 show ipv6 dhcp relay information option mac-format

Данная команда используется для отображения формата MAC-адреса в профиле и Option 37.

show ipv6 dhcp relay information option mac-format

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить формат MAC-адреса в профиле и Option 37.

Пример

В данном примере показано, как отобразить формат MAC-адреса в профиле Option 37.

```
Switch#show ipv6 dhcp relay information option mac-format

 Case              : Uppercase
 Delimiter         : Hyphen
 Delimiter Number  : 5
 Example             : AA-BB-CC-DD-EE-FF

Switch#
```

21.9 ipv6 dhcp relay remote-id udf

Используйте данную команду, чтобы настроить User Define Field (UDF) для Remote ID.

ipv6 dhcp relay remote-id udf {ascii *STRING* **| hex** *HEX-STRING***}**

Параметры

ascii *STRING*	Укажите строку ASCII для UDF Remote ID. Максимальное количество символов – 128.
hex *HEX-STRING*	Укажите шестнадцатеричную строку для UDF Remote ID. Максимальное количество знаков – 256.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить UDF для Remote ID.

Пример

В данном примере показано, как настроить UDF (строка ASCII) «PARADISE001».

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay remote-id udf ascii PARADISE001
Switch(config)#
```

В следующем примере показано, как настроить UDF (шестнадцатеричная строка ASCII) «010c08».

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay remote-id udf hex 010c08
Switch(config)#
```

21.10 ipv6 dhcp local-relay vlan

Данная команда используется для включения DHCPv6 Local Relay на VLAN или группе VLAN. Для отключения данной функции воспользуйтесь формой **no** этой команды.

ipv6 dhcp local-relay vlan *VLAN-ID* **[, | -]**
no ipv6 dhcp local-relay vlan *VLAN-ID* **[, | -]**

Параметры

VLAN-ID	Укажите VLAN или диапазон VLAN.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду для настройки функции DHCPv6 Local Relay.

Если функция DHCPv6 Local Relay включена, коммутатор добавит Option 37 и Option 18 в пакеты запроса клиента.

Если включена проверка Option 37, коммутатор проверит запрос от клиента и отбросит пакет, уже содержащий Option 37.

Если проверка Option 37 отключена, функция Local Relay будет добавлять Option 37 в пакет запроса вне зависимости от того, включена Option 37 или выключена.

Функция DHCPv6 Local Relay напрямую передаст пакет от сервера клиенту.

Пример

В данном примере показано, как включить функцию DHCPv6 Local Relay на VLAN 100.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp local-relay vlan 100
Switch(config)#
```

21.11 show ipv6 dhcp

Данная команда используется для отображения настроек DHCPv6 на интерфейсе.

show ipv6 dhcp [interface [*INTERFACE-ID***]]**

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейс VLAN, для которого необходимо отобразить настройки DHCPv6.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить DHCPv6 DUID устройства. Для отображения настроек DHCPv6 и информации об указанном интерфейсе VLAN используйте команду **show ipv6 dhcp interface**. Если ID интерфейса не указан, будут отображены все интерфейсы, для которых включена функция DHCPv6.

Пример

В данном примере показано, как отобразить настройки DHCPv6 для VLAN 1, если режим DHCPv6 Relay Mode включен.

```
Switch#show ipv6 dhcp interface vlan1

vlan1 is in relay mode
    Relay destinations:
      FE80::20A:BBFF:FECC:102 via vlan2

Switch#
```

В данном примере показано, как отобразить информацию о DHCPv6 для интерфейса VLAN 1, если режим DHCPv6 Mode отключен.

```
Switch#show ipv6 dhcp interface vlan1

Vlan1 is not in DHCPv6 mode

Switch#
```

21.12 show ipv6 dhcp relay information option

Данная команда используется для отображения настроек DHCPv6 Relay Information Options.

show ipv6 dhcp relay information option

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить настройки DHCPv6 Relay Information Options.

Пример

В данном примере показано, как отобразить настройки DHCPv6 Relay Remote ID.

```
Switch# show ipv6 dhcp relay information option

IPv6 DHCP relay remote-id
 Policy : drop
 Format : user-define
 UDF is ascii string “userstring”

Switch#
```

21.13 show ipv6 dhcp relay remote-id profile

Данная команда используется для отображения профилей Option 37.

show ipv6 dhcp relay remote-id profile

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить профили Option 37.

Пример

В данном примере показано, как отобразить профили Option 37.

```
Switch#show ipv6 dhcp relay remote-id profile

Option37 Profile name: profile1
Format string: "Ethernet %unit:/0/  %port:\:%sysname:%05svlan"


Total Entries:1

Switch#
```

21.14 show ipv6 dhcp relay information option format-type

Данная команда используется для отображения типа формата DHCPv6 Relay Information Options.

show ipv6 dhcp relay information option format-type [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить тип формата DHCPv6 Relay Information Options.

Пример

В данном примере показано, как отобразить тип формата DHCPv6 Relay Information Options.

```
Switch# show ipv6 dhcp relay information option format-type

 eth1/0/1
 Remote ID bind profile: 1

 Total Entries: 1
Switch#
```

22. Команды клиента D-Link Discovery Protocol (DDP)

22.1 ddp

Данная команда используется для того, чтобы включить функцию клиента DDP глобально или на указанных портах. Используйте форму **no**, чтобы отключить функцию клиента DDP.

ddp
no ddp

Параметры

Нет.

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode.

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и port-channel.
Используйте данную команду, чтобы включить/отключить функцию клиента DDP глобально или на физическом порту.

Если на порту отключена функция DDP, данный порт не будет ни обрабатывать, ни генерировать DDP-сообщения. Полученные портом DDP-сообщения распространяются в рамках широковещательного домена.

Пример

В данном примере показано, как включить DDP глобально.

```
Switch#configure terminal
Switch(config)#ddp
Switch(config)#
```

В следующем примере показано, как включить DDP на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ddp
Switch(config-if)#
```

22.2 ddp report-timer

Данная команда используется для настройки интервала между двумя последовательными сообщениями DDP report. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ddp report-timer {30 | 60 | 90 | 120 | Never}
no ddp report-timer

Параметры

30	Укажите, чтобы установить интервал 30 секунд.
60	Укажите, чтобы установить интервал 60 секунд.
90	Укажите, чтобы установить интервал 90 секунд.
120	Укажите, чтобы установить интервал 120 секунд.
Never	Укажите, чтобы не отправлять сообщения report.

По умолчанию

Параметр по умолчанию – **Never**.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить интервал между двумя последовательными сообщениями DDP report.

Пример

В данном примере показано, как установить интервал 60 секунд.

```
Switch#configure terminal
Switch(config)#ddp report-timer 60
Switch(config)#
```

22.3 show ddp

Данная команда используется для отображения настроек DDP на коммутаторе.

show ddp [interfaces *INTERFACE-ID* **[, | -]]**

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить информацию о DDP на коммутаторе.

Пример

В данном примере показано, как отобразить общую информацию о DDP.

```
Switch#show ddp

D-Link Discovery Protocol state: Enabled
DDP Version:  5
Report timer: Never

Switch#
```

В следующем примере показано, как отобразить информацию о DDP на интерфейсе Ethernet 1/0/1.

```
Switch#show ddp interface eth1/0/1

Interface         State
--------------    ----------
eth1/0/1          Enabled

Switch#
```

22.4 show ddp neighbors

Данная команда используется для отображения информации о соседних устройствах DDP.

show ddp neighbors [interface *INTERFACE-ID* **[, | -]] [detail]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите ID интерфейса для отображения.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
detail	(Опционально.) Укажите для отображения подробной информации.

По умолчанию
Нет.

Режим ввода команды
EXEC Mode.

Использование команды

Данная команда применяется для отображения информации о соседних устройствах DDP.

Пример
В данном примере показано, как отобразить информацию о соседних устройствах DDP.

```
Switch#show ddp neighbors
Total Entries: 2

Interface MAC Address       IP Address                              Product  DDP
                                                                    Category Ver
--------- ----------------- --------------------------------------- -------- ---
eth1/0/8  28-3B-82-7F-5A-08 10.90.90.90                             Switch   5
eth1/0/10 28-3B-82-AA-BB-CC 3FFE:22:33:44::55                       Switch   5

Switch#
```

Отображаемые параметры

Interface	Интерфейс, на котором получена и изучена запись.
MAC Address	MAC-адрес устройства.
IP Address	IPv4/IPv6-адрес устройства.
Product Category	Идентификация типа продукта. **Switch (Коммутатор)** **AP**: Access point (Точка доступа) **NC**: Network camera (Сетевая камера) **VE**: Video encoder (Видеокодер) **NVR**: Network video recorder (Сетевой видеорегистратор) **NAS**: Network attached storage (Сетевой накопитель) **SR**: Service router (Сервисный маршрутизатор) **WC**: Wireless controller (Беспроводной контроллер) **WS**: Wireless switch (Беспроводной коммутатор) **WR**: Wireless router (Беспроводной маршрутизатор) **EPOS**** **AAA-S**: AAA policy server (Сервер политики AAA) **DS**: Digital signage (Цифровая система оповещения) **NP**: Network printer (Сетевой принтер) **CNTRLER**: Controller (Контроллер)

DDP Ver	Версия протокола DDP.

В примере ниже показано, как отобразить подробную информацию о соседних устройствах DDP на интерфейсе Ethernet 1/0/8.

```
Switch#show ddp neighbors interface eth1/0/8 detail
Total Entries: 1

Interface: eth1/0/8
  MAC Address: 28-3B-82-7F-5A-08
  IP Address: 10.90.90.90
  Prefix Length: 24
  Model Name: DGS-3130-54TS
  DDP Version: 5
  Role: Client
  System Name: Switch-East1
  Product Category: Switch
  Firmware Version: 1.10.B024
  Hardware Version: A1
  Serial Number: DDLN7160002

Switch#
```

Отображаемые параметры

Interface	Интерфейс, на котором получена и изучена запись.
MAC Address	MAC-адрес устройства.
IP Address	IPv4/IPv6-адрес устройства.
Prefix Length	Длина префикса устройства.
Model Name	Модель устройства.
DDP Version	Версия протокола DDP.
Role	Назначение устройства DDP (сервер или клиент). Если назначение устройства – сервер или клиент V2, то будут отображены только параметры **Interface**, **MAC Address**, **IP Address**, **DDP Version** и **Role**.
System Name	Имя системы.
Product Category	Идентификация типа продукта, выполняется в сообщении DDP.
Firmware Version	Версия программного обеспечения устройства.
Hardware Version	Аппаратная версия устройства.
Serial Number	Серийный номер устройства.

23. Команды Domain Name System (DNS)

23.1 clear host

Данная команда используется для удаления динамически изученных записей узла в режиме Privileged User Mode.

clear host {all | [*HOST-NAME*]}

Параметры

all	Укажите, чтобы удалить все записи узла.
HOST-NAME	(Опционально.) Укажите, чтобы удалить указанную динамически изученную запись узла.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы удалить запись узла или все записи узла, которые динамически изучены DNS Resolver или Caching Server.

Пример

В данном примере показано, как удалить динамически изученную запись «www.abc.com» из таблицы узлов.

```
Switch#clear host www.abc.com
Switch#
```

23.2 ip domain lookup

Данная команда используется для включения DNS, что позволяет использовать функцию Domain Name Resolution. Для отключения данной функции воспользуйтесь формой **no** этой команды.

ip domain lookup
no ip domain lookup

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы включить функцию Domain Name Resolution. DNS Resolver отправляет запрос на указанный Name Server. Ответ, отсылаемый Name Server, будет кэширован и использован для ответа на последующие запросы.

Пример

В данном примере показано, как включить функцию Domain Name Resolution.

```
Switch#configure terminal
Switch(config)#ip domain lookup
Switch(config)#
```

23.3 ip host

Данная команда используется для настройки статической записи привязки для имени узла, а также IP-адреса в таблице узлов. Для удаления статической записи узла воспользуйтесь формой **no** данной команды.

ip host *HOST-NAME* **{***IP-ADDRESS* **|** *IPV6-ADDRESS***}**
no ip host *HOST-NAME* **{***IP-ADDRESS* **|** *IPV6-ADDRESS***}**

Параметры

HOST-NAME	Укажите имя узла устройства.
IP-ADDRESS	Укажите IPv4-адрес устройства.
IPV6-ADDRESS	Укажите IPv6-адрес устройства.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Имя узла, указанное в этой команде, должно быть подходящим.

Пример

В данном примере показано, как настроить запись привязки имени узла «www.abc.com» и IP-адреса 192.168.5.243.

```
Switch#configure terminal
Switch(config)#ip host www.abc.com 192.168.5.243
Switch(config)#
```

23.4 ip name-server

Данная команда используется для настройки IP-адреса Domain Name Server. Для удаления сконфигурированного DNS-сервера воспользуйтесь формой **no** этой команды.

ip name-server {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [{***IP-ADDRESS2* **|** *IPV6-ADDRESS2***}]**
no ip name-server {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [{***IP-ADDRESS2* **|** *IPV6-ADDRESS2***}]**

Параметры

IP-ADDRESS	Укажите IPv4-адрес Domain Name Server.
IPV6-ADDRESS	Укажите IPv6-адрес Domain Name Server.
IP-ADDRESS2	Укажите второй IPv4-адрес Domain Name Server.
IPV6-ADDRESS2	Укажите второй IPv6-адрес Domain Name Server.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы сконфигурировать DNS-сервер. Если система не может получить ответ от DNS-сервера, будет отправлен запрос на следующий сервер, и так до тех пор, пока ответ не будет получен. Если серверы Name Server уже сконфигурировны, то серверы, сконфигурированные позже, будут добавлены в список серверов. Можно указать два Name Server IPv4/IPv6.

Пример

В данном примере показано, как сконфигурировать Domain Name Server 192.168.5.134 и 5001:5::2.

```
Switch#configure terminal
Switch(config)#ip name-server 192.168.5.134 5001:5::2
Switch(config)#
```

23.5 ip name-server timeout

Данная команда используется для конфигурации значения тайм-аута для Name Server. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ip name-server timeout *SECONDS*
no ip name-server timeout

Параметры

SECONDS	Укажите максимальное время ожидания ответа от указанного Name Server. Диапазон значений: от 1 до 60 секунд.

По умолчанию

Значение по умолчанию – 3 секунды.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить максимальное значение времени ожидания ответа от указанного Name Server.

Пример

В данном примере показано, как указать значение тайм-аута 5 секунд.

```
Switch#configure terminal
Switch(config)#ip name-server timeout 5
Switch(config)#
```

23.6 show hosts

Данная команда используется для отображения настроек DNS.

show hosts

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить информацию о настройках DNS.

Пример

В данном примере показано, как отобразить информацию о настройках DNS.

```
Switch#show hosts

 Number of Static Entries:   1
 Number of Dynamic Entries:  0

 Host Name:          www.abc.com
 IP Address:         192.168.5.243
 Age:                forever


Switch#
```

23.7 show ip name-server

Данная команда используется для отображения настроек DNS.

show ip name-server

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить информацию о настройках DNS.

Пример

В данном примере показано, как отобразить информацию о настройках DNS.

```
Switch#show ip name-server

 Static name server:
 192.168.5.134
 5001:5::2

 Dynamic name server:

Switch#
```

24. Команды DoS Prevention

24.1 dos-prevention

Данная команда используется для включения и настройки механизма предотвращения атак DoS (DoS Prevention). Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

dos-prevention *DOS-ATTACK-TYPE*
no dos-prevention *DOS-ATTACK-TYPE*

Параметры

DOS-ATTACK-TYPE	Укажите строку, идентифицирующую тип DoS, который необходимо настроить.

По умолчанию

По умолчанию все поддерживаемые типы DoS отключены.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для включения и настройки механизма предотвращения DoS-атак определенного типа или всех поддерживаемых типов. Механизмы предотвращения атак DoS (сопоставление и принятие мер) являются функциями аппаратного обеспечения.

При включенном предотвращении атак DoS коммутатор сохранит событие (лог) в журнале, если был получен хотя бы один «атакующий» пакет.

Команда **no dos-prevention** с ключевым словом **all** используется для отключения механизма предотвращения атак DoS для всех поддерживаемых типов. Все настройки будут возвращены к значениям по умолчанию для определенных типов атак.

Следующие распространенные типы DoS-атак могут быть обнаружены большинством коммутаторов:

Blat: данный тип атаки включает в себя отправку устройству пакетов с портом источника TCP/ UDP, равным порту назначения. Это может послужить причиной того, что устройство будет отвечать самому себе.

Land: атака LAND включает в себя отправку устройству IP-пакетов с адресом источника и назначения, равным адресу устройства. Это может послужить причиной того, что устройство будет непрерывно отвечать самому себе.

TCP-NULL-scan: сканирование порта с использованием определенных пакетов, содержащих последовательность чисел от 0 и не содержащих флаги.

TCP-SYN-fin: сканирование порта с использованием определенных пакетов, содержащих флаги SYN и FIN.

TCP-SYN-SRCport-less-1024: сканирование порта с использованием определенных пакетов, содержащих порт источника 0-1023 и флаг SYN.

TCP-xmas-scan: сканирование порта с использованием определенных пакетов, содержащих последовательность чисел от 0 и флаги Urgent (URG), Push (PSH) и FIN.

Ping-death: данный тип атаки на компьютер включает в себя отправку некорректного или

вредоносного ping-запроса компьютеру. Обычно размер ping-запроса составляет 64 байта; многие компьютеры не могут распознать ping-запрос, если он больше, чем максимальный размер IP-пакета (65535 байт). Отправка ping-запроса такого размера может повредить компьютер назначения. Как правило, данным сбоем можно относительно просто воспользоваться. Отправка ping-пакета размером 65536 байт недопустима согласно сетевому протоколу, но пакет такого размера можно отправить, если он будет фрагментирован. При повторной сборке пакета буфер компьютера может переполниться, что послужит причиной сбоя системы.

TCP-tiny-frag: при атаке Tiny TCP Fragment используется фрагментация IP для создания очень маленьких фрагментов, чтобы TCP-заголовок был в отдельном фрагменте пакета. Это позволяет ему обойти проверку маршрутизатора и выполнить атаку.

All: все вышеперечисленные типы.

Пример

В данном примере показано, как включить механизм предотвращения атак DoS для атаки Land.

```
Switch#configure terminal
Switch(config)#dos-prevention land
Switch(config)#
```

В данном примере показано, как включить механизм предотвращения атак DoS для атак всех поддерживаемых типов.

```
Switch#configure terminal
Switch(config)#dos-prevention all
Switch(config)#
```

В данном примере показано, как отключить механизм предотвращения атак DoS для атак всех поддерживаемых типов.

```
Switch#configure terminal
Switch(config)#no dos-prevention all
Switch(config)#
```

24.2 show dos-prevention

Данная команда используется для получения информации о статусе предотвращения атак DoS.

show dos-prevention [*DOS-ATTACK-TYPE***]**

Параметры

DOS-ATTACK-TYPE	(Опционально.) Укажите тип DoS, который необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для получения информации о статусе предотвращения атак DoS.

Пример

В данном примере показано, как отобразить информацию о настройках предотвращения атак DoS.

```
Switch#show dos-prevention

DoS Prevention Information
DoS Type                    State
--------------------------- --------
Land Attack                 Disabled
Blat Attack                 Disabled
TCP Null                    Disabled
TCP Xmas                    Disabled
TCP SYN-FIN                 Disabled
TCP SYN SrcPort Less 1024   Disabled
Ping of Death Attack        Disabled
TCP Tiny Fragment Attack    Disabled

Switch#
```

В данном примере показано, как отобразить информацию о настройках предотвращения атак DoS.

```
Switch#show dos-prevention land

DoS Type : Land Attack
State    : Enabled

Switch#
```

24.3 snmp-server enable traps dos-prevention

Данная команда используется для отправки SNMP-уведомлений о DoS-атаках. Для отключения отправки SNMP-уведомлений воспользуйтесь формой **no** этой команды.

snmp-server enable traps dos-prevention
no snmp-server enable traps dos-prevention

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

При включенной функции предотвращения атак DoS коммутатор будет записывать событие в журнал каждые пять минут, если какой-либо атакующий пакет будет принят за этот промежуток времени.

Используйте данную команду, чтобы включить или отключить отправку уведомлений SNMP для таких событий.

Пример

В данном примере показано, как включить отправку trap-сообщений для атак DoS.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps dos-prevention
Switch(config)#
```

25. Команды Dynamic ARP Inspection

25.1 arp access-list

Данная команда используется для создания или изменения списка доступа ARP. Команда позволяет войти в режим ARP Access-list Configuration Mode. Для удаления списка доступа ARP воспользуйтесь формой **no** этой команды.

arp access-list *NAME*
no arp access-list *NAME*

Параметры

NAME	Укажите имя списка доступа ARP, который необходимо настроить. Максимальное количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Имя должно быть уникальным среди всех списков доступа. Имя чувствительно к регистру. В конце списка доступа указан запрет в доступе всем, кого нет в списке разрешений.

Пример

В данном примере показано, как настроить список доступа ARP с двумя разрешающими записями.

```
Switch#configure terminal
Switch(config)#arp access-list static-arp-list
Switch(config-arp-nacl)#permit ip 10.20.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)#permit ip 10.30.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)#
```

25.2 clear ip arp inspection log

Данная команда используется для очистки буфера журнала ARP Inspection.

clear ip arp inspection log

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для очистки буфера журнала ARP Inspection.

Пример

В данном примере показано, как очистить журнал ARP Inspection.

```
Switch#clear ip arp inspection log
Switch#
```

25.3 clear ip arp inspection statistics

Данная команда используется для удаления данных статистики Dynamic ARP Inspection.

clear ip arp inspection statistics {all | vlan *VLAN-ID* **[, | -]}**

Параметры

all	Укажите, чтобы удалить данные статистики Dynamic ARP Inspection для всех VLAN.
vlan *VLAN-ID*	Укажите VLAN или диапазон VLAN.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для удаления данных статистики Dynamic ARP Inspection.

Пример

В данном примере показано, как удалить данные статистики Dynamic ARP Inspection для VLAN 1.

```
Switch#clear ip arp inspection statistics vlan 1
Switch#
```

25.4 ip arp inspection filter vlan

Данная команда позволяет указать список доступа ARP, который будет использоваться для проверки ARP Inspection для VLAN. Для удаления указанной привязки воспользуйтесь формой **no** этой команды.

ip arp inspection filter *ARP-ACL-NAME* **vlan** *VLAN-ID* **[, | -] [static]**
no ip arp inspection filter *ARP-ACL-NAME* **vlan** *VLAN-ID* **[, | -] [static]**

Параметры

ARP-ACL-NAME	Укажите имя списка управления доступом. Максимальное количество символов – 32.
vlan *VLAN-ID*	Укажите VLAN, сопоставленную со списком доступа ARP.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
static	(Опционально.) Укажите при необходимости отбрасывать пакет, если пара привязки IP-to-Ethernet MAC не разрешена ARP ACL.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда применяется для указания списка доступа ARP, который будет использоваться для проверки ARP Inspection для VLAN. Для одной VLAN можно указать один список доступа.

Dynamic ARP Inspection проверяет ARP-пакеты, полученные в VLAN, для проверки корректности пары привязки IP-адреса источника и MAC-адреса источника. Во время проверки произойдет сопоставление адреса привязки и записей из таблицы привязок DHCP Snooping. Проверка будет производиться, если данная команда сконфигурирована.

Списки управления доступом ARP (ARP ACL) имеют более высокий приоритет над таблицей привязок DHCP Snooping. Если пакету явно запрещен доступ списком управления доступа, пакет будет отброшен. Если пакету неявно запрещен доступ, он будет дополнительно сопоставлен с записями привязки DHCP Snooping, если не указано ключевое слово «static». Если пакету неявно запрещен доступ и указано ключевое слово «static», пакет будет отброшен.

Пример

В данном примере показано, как применить список управления доступом ARP (ARP ACL) static ARP list в VLAN 10 для DAI.

```
Switch#configure terminal
Switch(config)#ip arp inspection filter static-arp-list vlan 10
Switch(config)#
```

25.5 ip arp inspection limit

Данная команда используется для ограничения скорости входящих ARP-запросов и ответов на интерфейсе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip arp inspection limit {rate *VALUE* **[burst interval** *SECONDS***] | none}**
no ip arp inspection limit

Параметры

rate *VALUE*	Укажите максимальное количество ARP-пакетов в секунду, которое может быть обработано. Диапазон значений: от 1 до 150.
burst interval *SECONDS*	(Опционально.) Укажите разрешенную величину продолжительности всплеска (burst duration) ARP-пакетов. Диапазон значений: от 1 до 15. Если не указано, значение по умолчанию составляет 1 секунду.
none	Укажите, чтобы скорость передачи ARP-пакетов не была ограничена.

По умолчанию

Для недоверенных интерфейсов DAI ограничение скорости составляет 15 пакетов в секунду с интервалом всплеска burst interval в 1 секунду.

Для доверенных интерфейсов DAI ограничений нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и port-channel.

Данная команда используется и для доверенных, и для недоверенных интерфейсов. Если скорость ARP-пакетов в секунду превышает ограничение и условия для настроенной продолжительности всплеска (burst duration), порт автоматически отключится из-за ошибки.

Пример

В данном примере показано, как назначить ограничение скорости входящих ARP-запросов до 30 пакетов в секунду и интервал проверки интерфейса до 5 следующих секунд.

```
Switch#configure terminal
Switch(config)#interface eth1/0/10
Switch(config-if)#ip arp inspection limit rate 30 burst interval 5
Switch(config-if)#
```

25.6 ip arp inspection log-buffer

Данная команда используется для настройки параметра буфера журнала ARP Inspection. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip arp inspection log-buffer entries *NUMBER*

no ip arp inspection log-buffer entries

Параметры

NUMBER	Укажите количество записей в буфере. Максимальное значение – 1024.

По умолчанию

Значение по умолчанию – 32.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для настройки максимального количества записей в буфере журнала. Буфер журнала ARP Inspection хранит информацию об ARP-пакетах. Первый пакет, прошедший проверку, будет отправлен в модуль системного журнала (syslog) и записан в буфер журнала проверки. Последующие пакеты из той же сессии не будут отправлены в модуль журнала, если только его запись в буфере журнала не будет удалена. Если буфер журнала полон, но события продолжают поступать, они не будут записаны в журнал. Если пользователь задает размер буфера меньше текущего номера записи, буфер журнала (лога) будет очищен автоматически.

Пример

В данном примере показано, как изменить размер буфера на 64.

```
Switch#configure terminal
Switch(config)#ip arp inspection log-buffer entries 64
Switch(config)#
```

25.7 ip arp inspection trust

Данная команда используется для назначения доверенного интерфейса для Dynamic ARP Inspection. Для отключения режима доверенного интерфейса воспользуйтесь формой **no** этой команды.

ip arp inspection trust

no ip arp inspection trust

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Если интерфейс находится в состоянии trust (доверенный), ARP-пакеты, поступающие на интерфейс, не будут проверяться. Если интерфейс находится в состоянии untrusted (недоверенный), ARP-пакеты, поступающие на порт и принадлежащие VLAN, в которой включена проверка, будут проверяться.

Пример

В данном примере показано, как настроить состояние Trust (доверенный) для интерфейса Ethernet 1/0/3 для DAI.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ip arp inspection trust
Switch(config-if)#
```

25.8 ip arp inspection validate

Данная команда используется для указания дополнительных проверок при ARP Inspection. Для отключения дополнительных проверок воспользуйтесь формой **no** этой команды.

ip arp inspection validate [src-mac] [dst-mac] [ip]

no ip arp inspection validate [src-mac] [dst-mac] [ip]

Параметры

src-mac	(Опционально.) Укажите для проверки пакетов ARP-запросов и ответов, а также согласованности MAC-адреса источника в заголовке Ethernet с MAC-адресом источника в заголовке ARP.
dst-mac	(Опционально.) Укажите для проверки пакетов ARP-ответов, а также согласованности MAC-адреса источника в заголовке Ethernet с MAC-адресом источника в заголовке ARP.
ip	(Опционально.) Укажите для проверки содержимого ARP на наличие недопустимых и непредвиденных IP-адресов. Укажите для проверки допустимости IP-адреса в заголовке ARP. Проверяются IP-адреса источника во всех ARP-запросах и ответах, и IP-адрес назначения в ARP-ответе. Пакеты, отправляемые на IP-адреса 0.0.0.0, 255.255.255.255 и все IP-адреса многоадресной рассылки отбрасываются. IP-адреса источника проверяются во всех ARP-запросах и ответах, а IP-адреса назначения проверяются только в ARP-ответах.

По умолчанию

По умолчанию данная опция отключена

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для указания дополнительных проверок во время Dynamic ARP Inspection. Указанные проверки будут производиться с пакетами, присылаемыми с недоверенных интерфейсов и принадлежащих VLAN, для которых включена IP ARP Inspection. Если параметры не указаны, все опции включены или выключены.

Пример

В данном примере показано, как включить проверку MAC-адреса источника.

```
Switch#configure terminal
Switch(config)#ip arp inspection validate src-mac
Switch(config)#
```

25.9 ip arp inspection vlan

Данная команда используется для включения Dynamic ARP Inspection для определенных VLAN. Для отключения Dynamic ARP Inspection для VLAN воспользуйтесь формой **no** этой команды.

ip arp inspection vlan *VLAN-ID* **[, | -]**
no ip arp inspection vlan *VLAN-ID* **[, | -]**

Параметры

VLAN-ID	Укажите VLAN, для которой необходимо включить или отключить функцию ARP Inspection.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию ARP Inspection отключена для всех VLAN.

Режим ввода команды

Global Configuration Mode.

Использование команды

Если VLAN включена для ARP Inspection, проверяться будут ARP-пакеты, включая пакеты ARP-запроса и ответа, принадлежащие VLAN и отправленные на недоверенный интерфейс. Если пара привязки IP-to-MAC MAC-адреса источника и IP-адреса источника не разрешены ARP ACL или таблицей привязок DHCP Snooping, ARP-пакеты будут отброшены. Помимо проверки привязки адреса, будет осуществляться дополнительная проверка, определяемая командой **ip arp inspection validate**.

Пример

В данном примере показано, как включить ARP Inspection в VLAN 2.

```
Switch#configure terminal
Switch(config)#ip arp inspection vlan 2
Switch(config)#
```

25.10 ip arp inspection vlan logging

Данная команда используется для управления типом пакетов, которые будут регистрироваться (логироваться). Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip arp inspection vlan *VLAN-ID* **[, | -] logging {acl-match {permit | all | none} | dhcp-bindings {permit | all | none}}**

no ip arp inspection vlan *VLAN-ID* **[, | -] logging {acl-match | dhcp-bindings}**

Параметры

VLAN-ID	Укажите VLAN, для которой необходимо включить или отключить функцию управления логированием.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
acl-match	Укажите критерии логирования для пакетов, отброшенных или разрешенных на основе совпадения со списком управления доступом (ACL).
acl-match permit	Укажите для логирования, разрешенного сконфигурированным списком управления доступом (ACL).
acl-match all	Укажите для логирования, разрешенного или запрещенного сконфигурированным списком управления доступом (ACL).
acl-match none	Укажите, чтобы отменить логирование пакетов на основе совпадения со списком управления доступом (ACL).
dhcp-bindings	Укажите критерии логирования для пакетов, отброшенных или разрешенных на основе совпадения с привязкой DHCP.
dhcp-bindings permit	Укажите для логирования, разрешенного привязкой DHCP.
dhcp-bindings all	Укажите для логирования, разрешенного или запрещенного привязкой DHCP.
dhcp-bindings none	Укажите, чтобы отменить логирование всех пакетов, разрешенных или запрещенных на основе привязки DHCP.

По умолчанию

По умолчанию пакеты **acl-match** and **dhcp-bindings** не логируются.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы указать критерии логирования для пакетов. При использовании команды **no** возврат к заводским настройкам параметров **acl-match** и **dhcp-bindings** необходимо настраивать отдельно.

Пример

В данном примере показано, как настроить ARP Inspection в VLAN 1 для добавления пакетов в журнал на основе списка управления доступом (ACL).

```
Switch#configure terminal
Switch(config)#ip arp inspection vlan 1 logging acl-match all
Switch(config)#
```

25.11 permit | deny (arp access-list)

Данная команда применяется для создания разрешающей или запрещающей ARP-записи. Для удаления записи воспользуйтесь формой **no** этой команды.

{permit | deny} ip {any | host *SENDER-IP* **|** *SENDER-IP SENDER-IP-MASK***} mac {any | host** *SENDER-MAC* **|** *SENDER-MAC SENDER-MAC-MASK***}**

no {permit | deny} ip {any | host *SENDER-IP* **|** *SENDER-IP SENDER-IP-MASK***} mac {any | host** *SENDER-MAC* **|** *SENDER-MAC SENDER-MAC-MASK***}**

Параметры

ip any	Укажите для сопоставления любого IP-адреса источника.
ip host *SENDER-IP*	Укажите для сопоставления единственного IP-адреса источника.
SENDER-IP SENDER-IP-MASK	Укажите для сопоставления группы IP-адресов источника с помощью битовой маски (bitmap). Проверяться будет бит, соответствующий значению бита 1. Формат ввода тот же, что и для IP-адреса.
mac any	Укажите для сопоставления любого MAC-адреса источника.
mac host *SENDER-MAC*	Укажите для сопоставления единственного MAC-адреса источника.
SENDER-MAC SENDER-MAC-MASK	Укажите для сопоставления группы MAC-адресов источника с помощью битовой маски (bitmap). Проверяться будет бит, соответствующий значению бита 1. Формат ввода тот же, что и для MAC-адреса.

По умолчанию

Нет.

Режим ввода команды

ARP Access-list Configuration Mode.

Использование команды

Используйте опцию **permit any**, чтобы команда разрешила доступ остальным пакетам, не прошедшим проверку по предыдущим правилам.

Пример

В данном примере показано, как настроить список доступа ARP с двумя разрешенными записями.

```
Switch#configure terminal
Switch(config)#arp access-list static-arp-list
Switch(config-arp-nacl)#permit ip 10.20.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)#permit ip 10.30.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)#
```

25.12 show ip arp inspection

Данная команда используется для отображения статуса DAI для указанного диапазона VLAN.

show ip arp inspection [interfaces [*INTERFACE-ID* **[, | -]] | statistics [vlan** *VLAN-ID* **[, | -]]]**

Параметры

interfaces	(Опционально.) Укажите интерфейс (порт) или диапазон интерфейсов (портов).
INTERFACE-ID	(Опционально.) Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
statistics	(Опционально.) Данные статистики DAI.
vlan *VLAN-ID*	(Опционально.) Укажите VLAN или группу VLAN.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется, чтобы отобразить статус DAI для указанного диапазона VLAN.

Пример

В данном примере показано, как включить отображение параметров статистики пакетов, которые были обработаны DAI для VLAN 10.

```
Switch#show ip arp inspection statistics vlan 10

VLAN    Forwarded    Dropped    DHCP Drops   ACL Drops
-----   ---------   ---------   ----------   ---------
10      21546       145261      145261       0
VLAN    DHCP Permits   ACL Permits   Source MAC Failures
-----   ------------   -----------   -------------------
10      21546           0            0
VLAN    Dest MAC Failures   IP Validation Failures
-----   -----------------   ----------------------
10      0                   0

Switch#
```

В данном примере показано, как включить отображение параметров статистики пакетов, которые были обработаны DAI для всех активных VLAN.

```
Switch#show ip arp inspection statistics

VLAN     Forwarded    Dropped     DHCP Drops    ACL Drops
-----    ---------    ---------   ----------    ---------
1        0            0           0             0
2        0            0           0             0
10       21546        145261      145261        0
100      0            0           0             0
200      0            0           0             0
1024     0            0           0             0
VLAN     DHCP Permits   ACL Permits   Source MAC Failures
-----    ------------   -----------   -------------------
1        0              0             0
2        0              0             0
10       21546          0             0
100      0              0             0
200      0              0             0
1024     0              0             0
VLAN     Dest MAC Failures   IP Validation Failures
-----    -----------------   ----------------------
1         0                        0
2         0                        0
10        0                        0
100       0                        0
200       0                        0
1024      0                        0

Switch#
```

Отображаемые параметры

VLAN	VLAN ID, на котором действует ARP Inspection.
Forwarded	Количество ARP-пакетов, переадресованных ARP Inspection.
Dropped	Количество ARP-пакетов, отброшенных ARP Inspection.
DHCP Drops	Количество ARP-пакетов, отброшенных таблицей DHCP Snooping.
ACL Drops	Количество ARP-пакетов, отброшенных с помощью ARP правил ACL (ARP ACL).
DHCP Permits	Количество ARP-пакетов, разрешенных таблицей привязок DHCP Snooping.
ACL Permits	Количество ARP-пакетов, разрешенных правилом ARP ACL.
Source MAC Failures	Количество ARP-пакетов, не прошедших проверку MAC-адреса источника.
Dest MAC Failures	Количество ARP-пакетов, не прошедших проверку MAC-адреса назначения.
IP Validation Failures	Количество ARP-пакетов, не прошедших проверку IP-адреса.

Пример

В данном примере показано, как включить отображение настроек и статус работы DAI.

```
Switch#show ip arp inspection

Source MAC Validation      : Disabled
Destination MAC Validation: Disabled
IP Address Validation      : Disabled
VLAN State    ACL Match                         Static ACL
---- -------- --------------------------------- ----------
2    Enabled  -                                 -
VLAN ACL Logging DHCP Logging
---- ----------- ------------
2    None        None

Switch#
```

Отображаемые параметры

VLAN	VLAN ID, на котором действует ARP Inspection.
Configuration	Состояние настроек ARP Inspection. **Enabled:** ARP Inspection работает. **Disabled:** ARP Inspection не работает.
ACL Match	Имя указанного списка управления доступом ARP (ARP ACL).
Static ACL	Настройки статического списка управления доступом (static ACL). **Yes**: статический список управления доступом (static ARP ACL) настроен. **No**: статический список управления доступом (static ARP ACL) не настроен.
ACL logging	Состояние логирования для пакетов, отброшенных или разрешенных на основе совпадения со списком управления доступом (ACL). **None**: пакеты, разрешенные списком управления доступом (ACL), не логируются. **Permit**: логирование происходит, если пакеты разрешены настроенным списком управления доступом (ACL). **Deny**: логирование происходит, если пакеты отброшены настроенным списком управления доступом (ACL). **All**: логирование для всех пакетов, разрешенных настроенным списком управления доступом (ACL).

DHCP Logging	Состояние логирования для пакетов, отброшенных или разрешенных на основе таблицы привязок DHCP. **None**: пакеты, отброшенные или разрешенные таблицей привязок DHCP, не логируются. **Permit**: логирование происходит, если пакеты разрешены таблицей привязок DHCP. **Deny**: логирование происходит, если пакеты отброшены таблицей привязок DHCP. **All**: пакеты, отброшенные или разрешенные таблицей привязок DHCP, логируются.

Пример

В данном примере показано, как включить отображение состояния для интерфейса Ethernet 1/0/3.

```
Switch#show ip arp inspection interfaces eth1/0/3

Interface       Trust State Rate(pps) Burst Interval
--------------- ----------- --------- --------------
eth1/0/3        untrusted   15        1
Total Entries: 1

Switch#
```

В данном примере показано, как включить отображение состояний для интерфейсов коммутатора.

```
Switch#show ip arp inspection interfaces eth1/0/1-7

Interface       Trust State Rate(pps) Burst Interval
--------------- ----------- --------- --------------
eth1/0/1        untrusted   15        1
eth1/0/2        untrusted   15        1
eth1/0/3        untrusted   15        1
eth1/0/4        untrusted   15        1
eth1/0/5        untrusted   15        1
eth1/0/6        untrusted   15        1
eth1/0/7        untrusted   15        1
Total Entries: 7

Switch#
```

Отображаемые параметры

Interface	Имя интерфейса, на котором работает ARP Inspection.
Trust State	Состояние интерфейса. **trusted:** данный интерфейс является доверенным портом ARP Inspection, все ARP-пакеты будут достоверны и не будут проходить авторизацию. **untrusted:** данный интерфейс является недоверенным портом ARP

	Inspection, все ARP-пакеты будут проходить авторизацию.
Rate (pps)	Верхняя граница количества входящих пакетов, обрабатываемых в секунду.
Burst Interval	Последовательный интервал в секундах, в течение которого на интерфейсе анализируется частота появления ARP-трафика.

25.13 show ip arp inspection log

Данная команда используется для отображения буфера лога (журнала) ARP Inspection.

show ip arp inspection log

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для отображения содержимого буфера лога (журнала) ARP Inspection.

Пример

В данном примере показано, как включить отображение буфера лога (журнала) ARP Inspection.

```
Switch#show ip arp inspection log
Total log buffer size: 32

Interface       VLAN Sender IP       Sender MAC        Occurrence
--------------- ---- --------------- ----------------- ----------------------
eth1/0/1        100  10.20.1.1       00-20-30-40-50-60 1 (2014-03-28 23:08:66)
eth1/0/2        100  10.5.10.16      55-66-20-30-40-50 2 (2014-04-02 00:11:54)
eth1/0/3        100  10.58.2.30      10-22-33-44-50-60 1 (2014-03-30 12:01:38)

Total Entries: 3

Switch#
```

Отображаемые параметры

Interface	Имя интерфейса, на котором производится логирование.
VLAN	VLAN, на которой производится логирование.
Sender IP	IP-адрес источника у логируемого ARP.

Sender MAC	MAC-адрес источника у логируемого ARP.
Occurence	Счетчик общего числа логирования записей, а также времени последнего логирования.

26. Команды Error Recovery

26.1 errdisable recovery

Данная команда используется для включения функции Error Recovery (автоматическое восстановление порта при возникновении ошибок), а также для настройки Recovery Interval (время восстановления). Используйте форму **no**, чтобы отключить опцию Auto-Recovery или вернуться к настройкам по умолчанию.

errdisable recovery cause {all | psecure-violation | storm-control | arp-rate | dhcp-rate | loopback-detect} [interval *SECONDS***]**

no errdisable recovery cause {all | psecure-violation | storm-control | arp-rate | dhcp-rate | loopback-detect} [interval]

Параметры

all	Укажите, чтобы включить опцию Auto-Recovery для всех ситуаций.
psecure-violation	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной Port Security Violation.
storm-control	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной Storm Control.
arp-rate	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной ARP Rate Limiting.
dhcp-rate	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной DHCP Rate Limiting.
loopback-detect	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной Loop Detection.
interval *SECONDS*	Укажите время, необходимое для восстановления порта при ошибке, вызванной указанным модулем. Доступный диапазон значений: от 5 до 86400 секунд. Значение по умолчанию – 300 секунд.

По умолчанию

По умолчанию опция Auto-Recovery отключена для всех ситуаций.

Режим ввода команды

Global Configuration Mode.

Использование команды

Ошибка на порту может быть вызвана такими событиями, как Port Security Violations, Storm Control и так далее. При возникновении ошибки порт отключается, однако для настроек конфигурации будет действовать опция **no shutdown**.

Восстановить порт при возникновении ошибки можно двумя способами. При помощи команды **errdisable recovery cause** администратор может включить функцию Auto-Recovery на портах,

отключенных при возникновении конкретных ошибок. Также порт можно восстановить вручную, для этого сначала введите команду **shutdown**, а затем **no shutdown**.

Пример

В данном примере показано, как установить Recovery Timer (таймер восстановления) на 200 секунд для восстановления порта при ошибке, вызванной Port Security Violation.

```
Switch#configure terminal
Switch(config)#errdisable recovery cause psecure-violation interval 200
Switch(config)#
```

В данном примере показано, как включить опцию Auto-Recovery для восстановления порта при ошибке, вызванной Port Security Violation.

```
Switch#configure terminal
Switch(config)#errdisable recovery cause psecure-violation
Switch(config)#
```

26.2 show errdisable recovery

Данная команда используется для отображения настроек Recovery Timer (таймер восстановления).

show errdisable recovery

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить настройки Recovery Timer.

Пример

В данном примере показано, как отобразить настройки Recovery Timer.

```
Switch# show errdisable recovery

ErrDisable Cause                    State         Interval
----------------------------------  ------------  -------------
Port Security                       enabled       200 seconds
Storm Control                       disabled      300 seconds
Dynamic ARP Inspection              disabled      300 seconds
DHCP Snooping                       disabled      300 seconds
Loop Detection                      disabled      300 seconds

Interfaces that will be recovered at the next timeout:

Switch#
```

26.3 snmp-server enable traps errdisable

Данная команда используется, чтобы включить отправку SNMP-уведомлений об ошибке на порту. Для отключения отправки SNMP-уведомлений воспользуйтесь формой **no** этой команды.

snmp-server enable traps errdisable [asserted] [cleared] [notification-rate *TRAP-RATE***]**
no snmp-server enable traps errdisable [asserted] [cleared] [notification-rate]

Параметры

asserted	(Опционально) Укажите, чтобы отправлять уведомления при возникновении ошибки на порту.
cleared	(Опционально) Укажите, чтобы отправлять уведомления при устранении ошибки на порту.
notification-rate *TRAP-RATE*	(Опционально.) Укажите количество trap-сообщений в минуту. Доступный диапазон значений: от 0 до 1000. Если количество пакетов превысило указанное значение, все последующие пакеты будут отброшены. Если указан 0, ограничения по количеству отсылаемых SNMP-уведомлений об ошибке в минуту отсутствуют.

По умолчанию

По умолчанию данная опция отключена.

Количество уведомлений в минуту по умолчанию – 0.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда с параметрами **asserted** и **cleared** включает или отключает уведомления об изменении ошибки на порту. При вводе команды с одним из параметров, будет включен или отключен только указанный тип уведомления. Состояние или значение другого типа уведомления не будут изменены.

Команды **snmp-server enable traps errdisable notification-rate** и **no snmp-server enable traps errdisable notification-rate** влияют только на настройку количества уведомлений в минуту, а не на состояние отправки уведомлений об ошибке на порту.

Пример

В данном примере показано, как включить отправку трапов при возникновении и устранении ошибки на порту, а также установить максимальное количество трапов в минуту равным 3.

```
Switch# configure terminal
Switch(config)#snmp-server enable traps errdisable asserted cleared notification-rate 3
Switch(config)#
```

27. Команды File System

27.1 delete

Данная команда используется для удаления файла.

delete *FILE-URL*

Параметры

FILE-URL	Укажите имя файла, который необходимо удалить.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Файл программного обеспечения или файл конфигурации, указанный в качестве загрузочного файла, удалить невозможно.

Пример

В данном примере показано, как удалить файл «Image2» из файловой системы внутренней памяти.

```
Switch#delete Image2
Delete Image2? (y/n) [n]  y
File is deleted.

Switch#
```

27.2 dir

Данная команда используется для отображения информации о файле или списке файлов в указанном пути.

dir [*URL***]**

Параметры

URL	(Опционально.) Укажите имя файла или каталога, который необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если путь не указан, будет использован текущий каталог. По умолчанию текущий каталог расположен в корне файловой системы внутренней памяти. Накопитель установлен в файловой системе и отображается пользователю в качестве подкаталога корневого каталога.

Используйте команду **dir** для корневого каталога, чтобы отобразить поддерживаемые файловые системы. Используйте команду **show storage media**, чтобы отобразить накопитель, привязанный к файловой системе.

Пример

В данном примере показано, как отобразить корневой каталог автономного коммутатора.

```
Switch#dir

Directory of /c:
1   -rw      21045792 Jan 01 2019 00:04:39  Image1
2   -rw      15720992 Jan 01 2019 00:06:39  Image2
3   -rw          1481 Jan 01 2019 00:02:07  Config1
4   d--             0 Jan 01 2019 00:02:07  system

66191360 bytes total (21315584 bytes free)

Switch#
```

27.3 show storage media-info

Данная команда используется для отображения информации о накопителе.

show storage media-info

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить информацию о доступных накопителях системы.

Пример

В данном примере показано, как отобразить информацию о доступных накопителях.

```
Switch#show storage media-info

Drive  Media Type  Size      FS-Type  Label
-----  ----------  --------  -------  -----------
c:     Flash       63 MB     swfs

Switch#
```

28. Команды Filter Database (FDB)

28.1 clear mac-address-table

Данная команда используется для удаления указанного динамического MAC-адреса, всех динамических MAC-адресов на указанном интерфейсе, всех динамических MAC-адресов на указанной VLAN или всех динамических MAC-адресов из таблицы MAC-адресов.

clear mac-address-table dynamic {all | address *MAC-ADDR* **| interface** *INTERFACE-ID* **| vlan** *VLAN-ID***}**

Параметры

all	Укажите, чтобы удалить все динамические MAC-адреса.
address *MAC-ADDR*	Укажите, чтобы удалить указанный динамический MAC-адрес.
interface *INTERFACE-ID*	Укажите интерфейс (физический порт или port-channel), на котором необходимо удалить MAC-адрес.
vlan *VLAN-ID*	Укажите VLAN ID в диапазоне от 1 до 4094.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы удалить записи динамических MAC-адресов. Будет удален только динамический индивидуальный адрес.

Пример

В данном примере показано, как удалить MAC-адрес 00:08:00:70:00:07 из таблицы динамических MAC-адресов.

```
Switch#clear mac-address-table dynamic address 00:08:00:70:00:07
Switch#
```

28.2 mac-address-table aging-time

Данная команда используется для настройки времени устаревания MAC-адресов в таблице. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

mac-address-table aging-time *SECONDS*

no mac-address-table aging-time

Параметры

SECONDS	Укажите время устаревания в диапазоне от 0 или 10 до 1000000 секунд. Укажите 0, чтобы отключить функцию устаревания MAC-адресов в таблице.

По умолчанию

Значение по умолчанию – 300 секунд.

Режим ввода команды

Global Configuration Mode.

Использование команды

Укажите время устаревания «0», чтобы отключить функцию устаревания MAC-адресов в таблице.

Пример

В данном примере показано, как указать значение времени устаревания 200 секунд.

```
Switch#configure terminal
Switch(config)#mac-address-table aging-time 200
Switch(config)#
```

28.3 mac-address-table learning

Данная команда используется, чтобы включить изучение MAC-адресов на физическом порту. Для отключения данной функции воспользуйтесь формой **no** этой команды.

mac-address-table learning interface *INTERFACE-ID* **[, | -]**

no mac-address-table learning interface *INTERFACE-ID* **[, | -]**

Параметры

INTERFACE-ID	Укажите интерфейс, который необходимо сконфигурировать.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.

Используйте данную команду, чтобы включить/отключить изучение MAC-адресов на физическом порту.

Пример

В данном примере показано, как включить опцию изучения MAC-адресов.

```
Switch#configure terminal
Switch(config)#mac-address-table learning interface eth1/0/5
Switch(config)#
```

28.4 mac-address-table notification change

Данная команда используется для включения/настройки функции уведомлений о MAC-адресах. Для отключения функции или возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

mac-address-table notification change [interval *SECONDS* **| history-size** *VALUE* **| trap-type {with-vlanid | without-vlanid}]**

no mac-address-table notification change [interval | history-size | trap-type]

Параметры

interval *SECONDS*	(Опционально.) Укажите интервал отправки trap-сообщений о MAC-адресах в диапазоне от 1 до 2147483647 секунд. Значение по умолчанию – 1 секунда.
history-size *VALUE*	(Опционально.) Укажите максимальное количество записей в таблице истории уведомлений. Доступный диапазон значений: от 0 до 500 записей. Значение по умолчанию – 1 запись.
trap-type	(Опционально.) Укажите, будет ли информация о trap-сообщении содержать VLAN ID.
with-vlanid	Укажите для включения VLAN ID в информацию о trap-сообщении.
without-vlanid	Укажите для исключения VLAN ID из информации о trap-сообщении.

По умолчанию

Уведомления о MAC-адресах отключены.
Интервал отправки trap-сообщений по умолчанию – 1 секунда.
Количество записей в таблице истории уведомлений по умолчанию – 1.
Тип trap-сообщения по умолчанию – without-vlanid.

Режим ввода команды

Global Configuration Mode.

Использование команды

При распознавании или удалении коммутатором MAC-адреса соответствующее уведомление может быть отправлено в таблицу истории уведомлений, а затем на SNMP-сервер, если запущена команда **snmp-server enable traps mac-notification change**. В таблице истории уведомлений хранятся

распознанные или удаленные MAC-адреса тех интерфейсов, для которых включены trap-сообщения. Для групповых адресов события не генерируются.

Пример

В данном примере показано, как включить уведомления об изменении MAC-адреса и установить интервал 10 секунд, а лимит по количеству записей в истории – 500.

```
Switch#configure terminal
Switch(config)#mac-address-table notification change
Switch(config)#mac-address-table notification change interval 10
Switch(config)#mac-address-table notification change history-size 500
Switch(config)#
```

28.5 mac-address-table static

Данная команда используется для добавления статического адреса в таблицу MAC-адресов. Для удаления записи из таблицы воспользуйтесь формой **no** этой команды.

mac-address-table static *MAC-ADDR* **vlan** *VLAN-ID* **{interface** *INTERFACE-ID* **[, | -] | drop}**

no mac-address-table static {all | *MAC-ADDR* **vlan** *VLAN-ID* **[interface** *INTERFACE-ID***] [, | -]}**

Параметры

MAC-ADDR	Укажите индивидуальный или групповой MAC-адрес. Пакеты с адресом назначения (destination), соответствующим данному MAC-адресу, полученные указанной VLAN, будут направлены на указанный интерфейс.
vlan *VLAN-ID*	Укажите VLAN записи в диапазоне от 1 до 4094.
interface *INTERFACE-ID*	Укажите порты продвижения кадров.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
drop	Укажите, чтобы отбросить кадры, отправленные с указанного MAC-адреса / на указанный MAC-адрес на обозначенной VLAN.
all	Укажите, чтобы удалить все записи статических MAC-адресов.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Для записи индивидуального MAC-адреса можно указать только один интерфейс. Для записи группового MAC-адреса можно указать несколько интерфейсов. Чтобы удалить запись индивидуального MAC-адреса, interface ID указывать не нужно. При удалении записи группового MAC-адреса будет удален только тот интерфейс, ID которого указан. Если interface ID не указан, будет удалена вся запись группового MAC-адреса. Параметр **drop** может быть применен только для записи индивидуального MAC-адреса.

Пример

В данном примере показано, как добавить статический адрес C2:F3:22:0A:12:F4 в таблицу MAC-адресов. Если пакет с MAC-адресом назначения C2:F3:22:0A:12:F4 получен на VLAN 4, он будет направлен на интерфейс Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#mac-address-table static C2:F3:22:0A:12:F4 vlan 4 interface eth1/0/1
Switch(config)#
```

28.6 multicast filtering-mode

Данная команда используется, чтобы настроить способ обработки групповых пакетов для VLAN. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

multicast filtering-mode {forward-all | forward-unregistered | filter-unregistered}

no multicast filtering-mode

Параметры

forward-all	Укажите, чтобы распространить все групповые пакеты на основании VLAN-домена.
forward-unregistered	Укажите, чтобы направить зарегистрированные групповые пакеты на основании таблицы переадресации и распространить все незарегистрированные групповые пакеты на основании VLAN-домена.
filter-unregistered	Укажите, чтобы направить зарегистрированные пакеты на основании таблицы переадресации и отфильтровать все незарегистрированные групповые пакеты.

По умолчанию

Параметр по умолчанию – **forward-unregistered**.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Данный режим фильтрации применим только к групповым пакетам, предназначенным для адресов, незарезервированных для групповых адресов.

Пример

В данном примере показано, как установить режим фильтрации групповых пакетов на VLAN 100, чтобы отфильтровать незарегистрированные адреса.

```
Switch#configure terminal
Switch(config)#vlan 100
Switch(config-vlan)#multicast filtering-mode filter-unregistered
Switch(config-vlan)#
```

28.7 show mac-address-table

Данная команда используется для отображения записи указанного MAC-адреса или записей MAC-адреса для указанного интерфейса/VLAN.

show mac-address-table [dynamic | static] [address *MAC-ADDR* **| interface** *INTERFACE-ID* **| vlan** *VLAN-ID***]**

Параметры

dynamic	(Опционально.) Укажите, чтобы отобразить только записи таблицы динамических MAC-адресов.
static	(Опционально.) Укажите, чтобы отобразить только записи таблицы статических MAC-адресов.
address *MAC-ADDR*	(Опционально.) Укажите 48-битный MAC-адрес.
interface *INTERFACE-ID*	(Опционально.) Укажите, чтобы отобразить информацию для указанного интерфейса (физического порта или port-channel).
vlan *VLAN-ID*	(Опционально.) Укажите VLAN ID в диапазоне от 1 до 4094.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

При указании параметра **interface** будет отображена индивидуальная запись, чей интерфейс передачи соответствует указанному интерфейсу.

Пример

В данном примере показано, как отобразить все записи таблицы MAC-адресов для MAC-адреса 00-02-4b-28-c4-82.

```
Switch# show mac-address-table address 00:02:4B:28:C4:82

VLAN    MAC Address        Type    Ports
------ ----------------- -------- --------
1      00-02-4B-28-C4-82   Static   CPU

Total Entries: 1

Switch#
```

В данном примере показано, как отобразить все записи таблицы статических MAC-адресов.

```
Switch# show mac-address-table static
VLAN    MAC Address          Type     Ports
---------------------------------------
1     00-02-4B-28-C4-82     Static    CPU
2     00-02-4B-28-C4-82     Static    CPU
4     00-01-00-02-00-04     Static    eth1/0/2
4     C2-F3-22-0A-12-F4     Static    port-channel2
6     00-01-00-02-00-07     Static    eth1/0/1
6     00-01-00-02-00-10     Static    Drop

Total Entries : 6

Switch#
```

В данном примере показано, как отобразить все записи таблицы MAC-адресов для VLAN 1.

```
Switch# show mac-address-table vlan 1

VLAN   MAC Address          Type         Ports
-----------------------------------------------
1     00-02-4B-28-C4-82    Static        CPU
1     00-03-40-11-22-33    Dynamic       eth1/0/2

Total Entries: 2

Switch#
```

28.8 show mac-address-table aging-time

Данная команда используется для отображения времени устаревания MAC-адресов в таблице.

show mac-address-table aging-time

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить время устаревания MAC-адресов в таблице.

Пример

В данном примере показано, как отобразить время устаревания MAC-адресов в таблице.

```
Switch#show mac-address-table aging-time

Aging Time is 300 seconds

Switch#
```

28.9 show mac-address-table learning

Данная команда используется для отображения статуса изучения MAC-адресов.

show mac-address-table learning [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейс, который необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если не указаны дополнительные параметры, будут отображены все физические порты.

Пример

В данном примере показано, как отобразить статус изучения MAC-адресов на всех физических портах от 1 до 10.

```
Switch#show mac-address-table learning interface eth1/0/1-10

Port                        State
--------------------------  --------
eth1/0/1                    Enabled
eth1/0/2                    Enabled
eth1/0/3                    Enabled
eth1/0/4                    Enabled
eth1/0/5                    Enabled
eth1/0/6                    Enabled
eth1/0/7                    Enabled
eth1/0/8                    Enabled
eth1/0/9                    Enabled
eth1/0/10                   Enabled

Switch#
```

28.10 show mac-address-table notification change

Данная команда используется для отображения настроек уведомлений о MAC-адресах или истории уведомлений.

show mac-address-table notification change [interface [*INTERFACE-ID*] | history]

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейс, который необходимо отобразить.
history	(Опционально.) Укажите, чтобы отобразить историю уведомлений об изменении MAC-адреса.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если не указаны дополнительные параметры, будут отображены общие настройки. Используйте параметр **interface**, чтобы отобразить информацию обо всех интерфейсах. Чтобы отобразить конкретный интерфейс, введите его ID.

Пример

В данном примере показано, как отобразить настройки уведомлений об изменении MAC-адреса на всех интерфейсах.

```
Switch# show mac-address-table notification change interface

Interface                Added Trap       Removed Trap
-----------------------  -------------    -------------

eth1/0/1                 Disabled         Disabled
eth1/0/2                 Disabled         Disabled
eth1/0/3                 Disabled         Disabled
eth1/0/4                 Disabled         Disabled
eth1/0/5                 Disabled         Disabled
eth1/0/6                 Disabled         Disabled
eth1/0/7                 Disabled         Disabled
eth1/0/8                 Disabled         Disabled
eth1/0/9                 Disabled         Disabled
eth1/0/10                Disabled         Disabled
eth1/0/11                Disabled         Disabled
eth1/0/12                Disabled         Disabled
eth1/0/13                Disabled         Disabled
eth1/0/14                Disabled         Disabled
eth1/0/15                Disabled         Disabled
eth1/0/16                Disabled         Disabled
eth1/0/17                Disabled         Disabled
eth1/0/18                Disabled         Disabled
eth1/0/19                Disabled         Disabled
eth1/0/20                Disabled         Disabled
eth1/0/21                Disabled         Disabled
eth1/0/22                Disabled         Disabled
eth1/0/23                Disabled         Disabled
eth1/0/24                Disabled         Disabled
eth1/0/25                Disabled         Disabled
eth1/0/26                Disabled         Disabled
eth1/0/27                Disabled         Disabled
eth1/0/28                Disabled         Disabled

Switch#
```

В данном примере показано, как отобразить общие настройки уведомлений о MAC-адресах.

```
Switch#show mac-address-table notification change

MAC Notification Change Feature: Enabled
Interval between Notification Traps: 10 seconds
Maximum Number of Entries Configured in History Table: 500
Current History Table Length: 0
MAC Notification Trap State: Disabled
Trap Type: Without VID

Switch#
```

В данном примере показано, как отобразить историю уведомлений о MAC-адресах.

```
Switch#show mac-address-table notification change history

History Index: 1
Operation:ADD Vlan: 1 MAC Address: 00-f8-d0-12-34-56 eth1/0/1
History Index: 2
Operation:DEL Vlan: 1 MAC Address: 00-f8-d0-00-00-01 eth1/0/1
History Index: 3
Operation:DEL Vlan: 1 MAC Address: 00-f8-d0-00-00-02 eth1/0/1

Switch#
```

28.11 show multicast filtering-mode

Данная команда используется для отображения режима фильтрации при обработке групповых пакетов, полученных на интерфейсе.

show multicast filtering-mode [interface *VLAN-ID***]**

Параметры

interface *VLAN-ID*	(Опционально.) Укажите VLAN, которую необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить режим фильтрации при обработке групповых пакетов, полученных на интерфейсе.

Пример

В данном примере показано, как отобразить настройки режима фильтрации групповых пакетов для всех VLAN.

```
Switch#show multicast filtering-mode

Interface                        Layer 2 Multicast Filtering Mode
-------------------------------  --------------------------------
default                          forward-unregistered

Total Entries: 1

Switch#
```

28.12 snmp-server enable traps mac-notification change

Данная команда используется для включения отправки SNMP trap об уведомлениях MAC. Для отключения функции воспользуйтесь формой **no** этой команды.

snmp-server enable traps mac-notification change
no snmp-server enable traps mac-notification change

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы включить/отключить отправку SNMP trap об уведомлениях MAC.

Пример

В данном примере показано, как включить отправку SNMP trap об уведомлениях MAC.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps mac-notification change
Switch(config)#
```

28.13 snmp trap mac-notification change

Данная команда используется для включения уведомлений об изменении MAC-адреса на указанном интерфейсе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

snmp trap mac-notification change {added | removed}
no snmp trap mac-notification change {added | removed}

Параметры

added	Укажите, чтобы включить уведомления об изменении MAC-адреса при добавлении MAC-адреса на интерфейс.
removed	Укажите, чтобы включить уведомления об изменении MAC-адреса при удалении MAC-адреса с интерфейса.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Даже если при помощи команды **snmp trap mac-notification change** на интерфейсе включена отправка уведомлений, уведомления будут отправлены в таблицу истории только при использовании команды **mac-address-table notification change**.

Пример

В данном примере показано, как включить уведомления о добавлении MAC-адреса на интерфейсе Ethernet 1/0/2.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#snmp trap mac-notification change added
Switch(config-if)#
```

29. Команды Gratuitous ARP

29.1 ip arp gratuitous

Данная команда используется, чтобы включить изучение пакетов Gratuitous ARP в таблице ARP-кэша. Для отключения ARP control воспользуйтесь формой no этой команды.

ip arp gratuitous
no ip arp gratuitous

Параметры

Нет.

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode.

Использование команды

По умолчанию система изучает пакеты Gratuitous ARP в таблице ARP-кэша.

Пример

В данном примере показано, как отключить изучение пакетов Gratuitous ARP Request.

```
Switch#configure terminal
Switch(config)#no ip arp gratuitous
Switch(config)#
```

29.2 ip gratuitous-arps

Данная команда используется, чтобы включить передачу пакетов Gratuitous ARP Request. Для отключения передачи воспользуйтесь формой **no** этой команды.

ip gratuitous-arps [dad-reply]
no ip gratuitous-arps [dad-reply]

Параметры

dad-reply	(Опционально.) Укажите, будет ли система высылать ответный пакет Gratuitous ARP Request с Broadcast DA при получении пакета Gratuitous ARP Request и обнаружении дублированного IP-адреса.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Пакет Gratuitous ARP Request – это пакет запроса ARP, где IP-адрес источника (source) и IP-адрес назначения (destination) являются IP-адресом передающего устройства, а MAC-адрес назначения – широковещательным адресом.

Устройство использует пакет Gratuitous ARP Request, чтобы определить, дублирован ли IP-адрес другими узлами, или выполнить предварительную загрузку / перенастроить конфигурацию записи ARP-кэша узлов, подключенных к интерфейсу.

Используйте команду **ip gratuitous-arps**, чтобы включить передачу запроса Gratuitous ARP. Устройство вышлет пакет, если IP-интерфейс в состоянии link-up или если IP-адрес интерфейса сконфигурирован/изменен.

Используйте команду **ip gratuitous-arps dad-reply**, чтобы включить передачу запросов Gratuitous ARP. Устройство вышлет пакет при обнаружении дублированного IP-адреса.

Пример

В данном примере показано, как отправлять сообщения Gratuitous ARP.

```
Switch#configure terminal
Switch(config)#ip gratuitous-arps dad-reply
Switch(config)#
```

29.3 arp gratuitous-send interval

Данная команда используется для установки интервала отправки сообщений Gratuitous ARP Request на интерфейсе. Для отключения функции воспользуйтесь формой **no** этой команды.

arp gratuitous-send interval *SECONDS*
no arp gratuitous-send

Параметры

SECONDS	Укажите временной интервал для отправки сообщений с Gratuitous ARP Request. Доступный диапазон значений: от 0 до 3600. Если указан 0, данная опция отключена.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Если интерфейс коммутатора используется в качестве шлюза для конечных устройств и у данных устройств наблюдается поведение ложного шлюза, администратор может настроить регулярную отправку сообщений с Gratuitous ARP Request на данном интерфейсе для уведомления о том, что коммутатор является подлинным шлюзом.

Пример

В данном примере показано, как включить отправку сообщений Gratuitous ARP.

```
Switch#configure terminal
Switch(config)#ip gratuitous-arps
Switch(config)#interface vlan100
Switch(config-if)#arp gratuitous-send interval 1
Switch(config-if)#
```

29.4 snmp-server enable traps gratuitous-arp

Данная команда используется, чтобы включить отправку SNMP-уведомлений об обнаружении дублированного IP-адреса Gratuitous ARP. Для отключения функции воспользуйтесь формой **no** этой команды.

snmp-server enable traps gratuitous-arp

no snmp-server enable traps gratuitous-arp

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для включения/отключения отправки SNMP-уведомлений об обнаружении дублированного IP-адреса Gratuitous ARP.

Пример

В данном примере показано, как включить отправку SNMP-уведомлений об обнаружении дублированного IP-адреса Gratuitous ARP.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps gratuitous-arp
Switch(config)#
```

30. Команды управления интерфейсом

30.1 clear counters

Данная команда используется для сброса счетчиков интерфейсов.

clear counters {all | interface *INTERFACE-ID* **[, | -]}**

Параметры

all	Укажите, если необходимо сбросить счетчики для всех интерфейсов.
interface *INTERFACE-ID*	Укажите интерфейсы, которые необходимо удалить. Параметр применим для физических портов.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте команду, чтобы сбросить счетчики для интерфейсов.

Пример

В данном примере показано, как сбросить счетчики для интерфейса Ethernet 1/0/1.

```
Switch#clear counters interface eth1/0/1
Switch#
```

30.2 description

Данная команда используется для добавления описания на интерфейс. Для удаления описания воспользуйтесь формой **no** этой команды.

description *STRING*
no description

Параметры

STRING	Описание интерфейса. Максимально допустимое количество символов – 64.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применяется для добавления описания на предварительно заданные типы интерфейса. Указанное описание соответствует объекту MIB «ifAlias», определенному в RFC 2233.

Пример

В данном примере показано, как добавить описание «Physical Port 10» на интерфейс Ethernet 1/0/10.

```
Switch#configure terminal
Switch(config)#interface eth1/0/10
Switch(config-if)#description Physical Port 10
Switch(config-if)#
```

В данном примере показано, как добавить описание «Data VLAN» на виртуальный LAN-интерфейс второго уровня.

```
Switch# configure terminal
Switch(config)#interface l2vlan 1
Switch(config-if)#description Data VLAN
Switch(config-if)#
```

30.3 interface

Данная команда используется для входа в режим Interface Configuration Mode для одного интерфейса. Для удаления интерфейса воспользуйтесь формой **no** этой команды.

interface *INTERFACE-ID*
no interface *INTERFACE-ID*

Параметры

INTERFACE-ID	Укажите ID интерфейса (Interface ID). В качестве ID интерфейса указывается тип и номер интерфейса. Типы интерфейса указаны ниже: **Ethernet** – физический Ethernet-порт коммутатора; **L2vlan** – интерфейс VLAN уровня 2 на основе IEEE 802.1Q; **Port-channel** – агрегированный интерфейс port-channel; **Vlan** – интерфейс VLAN.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для входа в режим Interface Configuration Mode для определенного интерфейса. Формат номера интерфейса зависит от типа интерфейса. Для интерфейсов физических портов пользователь не может войти в интерфейс, если порт коммутатора не существует. Интерфейс физического порта не может быть удален командой **no**.

Используйте команду **interface vlan** для создания интерфейса 3 уровня. Используйте команду **vlan** в режиме Global Configuration Mode, чтобы создать VLAN перед созданием интерфейса 3 уровня. Используйте команду **no interface vlan**, чтобы удалить интерфейс 3 уровня.

Интерфейс port-channel создается автоматически, когда для настройки интерфейса физического порта используется команда **channel-group**. Интерфейс port-channel будет удален автоматически, если интерфейс физического порта для команды **channel-group** не будет настроен. Используйте команду **no interface port-channel**, чтобы удалить port-channel.

Режим интерфейса **l2vlan** используется только для добавления описания к существующим L2VLAN. Команда **interface l2vlan** не создает новые интерфейсы, а форма **no** данной команды не удаляет существующие интерфейсы.

Пример

В данном примере показано, как войти в режим Interface Configuration Mode для интерфейса Ethernet 1/0/5.

```
Switch#configure terminal
Switch(config)#interface eth1/0/5
Switch(config-if)#
```

В данном примере показано, как войти в режим Interface Configuration Mode для VLAN 100.

```
Switch#configure terminal
Switch(config)#interface vlan100
Switch(config-if)#
```

В данном примере показано, как войти в режим Interface Configuration Mode для port-channel 3.

```
Switch#configure terminal
Switch(config)#interface port-channel3
Switch(config-if)#
```

30.4 interface range

Данная команда позволяет войти в режим Interface Range Configuration Mode для нескольких интерфейсов.

interface range *INTERFACE-ID* **[, | -]**

Параметры

INTERFACE-ID	Укажите ID интерфейса. В качестве ID интерфейса указывается тип и номер интерфейса. Типы интерфейса указаны ниже: **Ethernet** – физический Ethernet-порт коммутатора; **L2vlan** – интерфейс VLAN уровня 2 на основе IEEE 802.1Q.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Команда используется для входа в режим Interface Range Configuration Mode для указанного диапазона интерфейсов. Команды, введенные в режиме Interface Range Configuration Mode, применяются ко всем интерфейсам указанного диапазона.

Пример

В данном примере показано, как войти в режим Interface Range Configuration Mode для диапазона интерфейсов от Ethernet 1/0/1 до 1/0/5, а также для интерфейса Ethernet 1/0/8.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/1-5,1/0/8
Switch(config-if-range)#
```

30.5 show counters

Данная команда используется для отображения информации об интерфейсе.

show counters [interface *INTERFACE-ID* **[- | ,]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейс, который необходимо отобразить. Если интерфейс не указан, будут отображаться счетчики для всех интерфейсов. Параметр применим для физических портов.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.

-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется, чтобы отобразить статистику счетчиков для указанного интерфейса/интерфейсов.

Пример

В данном примере показано, как включить отображение счетчиков для интерфейса Ethernet 1/0/1.

```
Switch#show counters interface eth1/0/1

eth1/0/1 counters
rxHCTotalPkts                    : 1549
txHCTotalPkts                    : 154322
rxHCUnicastPkts                  : 1319
txHCUnicastPkts                  : 473
rxHCMulticastPkts                : 78
txHCMulticastPkts                : 78572
rxHCBroadcastPkts                : 152
txHCBroadcastPkts                : 75277
rxHCOctets                       : 135984
txHCOctets                       : 16607644
rxHCPkt64Octets                  : 244
rxHCPkt65to127Octets             : 1176
rxHCPkt128to255Octets            : 110
rxHCPkt256to511Octets            : 15
rxHCPkt512to1023Octets           : 3
rxHCPkt1024to1518Octets          : 1
rxHCPkt1519to1522Octets          : 0
rxHCPkt1519to2047Octets          : 0
rxHCPkt2048to4095Octets          : 0
rxHCPkt4096to9216Octets          : 0
rxHCPkt9217to16383Octets         : 0
txHCPkt64Octets                  : 132105
txHCPkt65to127Octets             : 1531
txHCPkt128to255Octets            : 2120
txHCPkt256to511Octets            : 13794
txHCPkt512to1023Octets           : 4712
```

```
txHCPkt1024to1518Octets          : 60
txHCPkt1519to1522Octets          : 0
txHCPkt1519to2047Octets          : 0
txHCPkt2048to4095Octets          : 0
txHCPkt4096to9216Octets          : 0
txHCPkt9217to16383Octets         : 0

rxCRCAlignErrors                 : 0
rxUndersizedPkts                 : 0
rxOversizedPkts                  : 0
rxFragmentPkts                   : 0
rxJabbers                        : 0
rxSymbolErrors                   : 0
rxBufferFullDropPkts             : 0
rxACLDropPkts                    : 0
rxMulticastDropPkts              : 0
rxVLANIngressCheckDropPkts       : 0
rxIpv6DropPkts                   : 0
rxSTPDropPkts                    : 0
rxStormAndTableDropPkts          : 0
rxMTUDropPkts                    : 0

txCollisions                     : 0
ifInErrors                       : 0
ifOutErrors                      : 0
ifInDiscards                     : 0
ifOutDiscards                    : 0
ifInUnknownProtos                : 0
txDelayExceededDiscards          : 0
txCRC                            : 0
txSTPDropPkts                    : 0
txHOLDropPkts                    : 0
txCoS0DropPkts                   : 0
txCoS1DropPkts                   : 0
txCoS2DropPkts                   : 0
txCoS3DropPkts                   : 0
txCoS4DropPkts                   : 0
txCoS5DropPkts                   : 0
txCoS6DropPkts                   : 0
txCoS7DropPkts                   : 0
```

```
dot3StatsAlignmentErrors           : 0
dot3StatsFCSErrors                 : 0
dot3StatsSingleColFrames           : 0
dot3StatsMultiColFrames            : 0
dot3StatsSQETestErrors             : 0
dot3StatsDeferredTransmissions     : 0
dot3StatsLateCollisions            : 0
dot3StatsExcessiveCollisions       : 0
dot3StatsInternalMacTransmitErrors : 0
dot3StatsCarrierSenseErrors        : 0
dot3StatsFrameTooLongs             : 0
dot3StatsInternalMacReceiveErrors  : 0

linkChange                         : 5


Switch#
```

Отображаемые параметры

rxHCTotalPkts	Счетчик принятых пакетов. Увеличивается с каждым принятым пакетом (включая поврежденные пакеты, все одноадресные, широковещательные и многоадресные пакеты, а также пакеты управления MAC).
txHCTotalPkts	Счетчик переданных пакетов. Увеличивается с каждым переданным пакетом (включая поврежденные пакеты, все одноадресные, широковещательные и многоадресные пакеты, а также пакеты управления MAC).
rxHCUnicastPkts	Счетчик принятых пакетов одноадресной рассылки. Увеличивается с каждым успешно принятым пакетом одноадресной рассылки.
txHCUnicastPkts	Счетчик переданных пакетов одноадресной рассылки. Увеличивается с каждым успешно переданным пакетом одноадресной рассылки.
rxHCMulticastPkts	Счетчик принятых пакетов многоадресной рассылки. Увеличивается с каждым успешно принятым пакетом многоадресной рассылки (за исключением пакетов управления MAC).
txHCMulticastPkts	Счетчик переданных пакетов многоадресной рассылки. Увеличивается с каждым успешно переданным пакетом многоадресной рассылки (за исключением пакетов управления MAC).
rxHCBroadcastPkts	Счетчик принятых пакетов широковещательной рассылки. Увеличивается с каждым успешно принятым пакетом широковещательной рассылки.

txHCBroadcastPkts	Счетчик переданных пакетов широковещательной рассылки. Увеличивается с каждым успешно переданным пакетом широковещательной рассылки.
rxHCOctets	Счетчик принятых байтов. Увеличивается с подсчетом байтов принятых пакетов, включая поврежденные пакеты (за исключением битов кадров, но включая байты FCS). **Примечание**: для усеченного пакета счетчик учитывает только размер max-rcv-frame.
txHCOctets	Счетчик переданных байтов. Увеличивается с подсчетом байтов переданных пакетов (за исключением битов кадров, но включая байты FCS).
rxHCPkt64Octets	Счетчик принятых 64-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type) до 64 байт включительно (за исключением битов кадров, но включая байты FCS).
rxHCPkt65to127Octets	Счетчик принятых 65 – 127-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type) от 65 до 127 байт включительно (за исключением битов кадров, но включая байты FCS).
rxHCPkt128to255Octets	Счетчик принятых 128 – 255-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type) от 128 до 255 байт включительно (за исключением битов кадров, но включая байты FCS).
rxHCPkt256to511Octets	Счетчик принятых 256 – 511-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type) от 256 до 511 байт включительно (за исключением битов кадров, но включая байты FCS).
rxHCPkt512to1023Octets	Счетчик принятых 512 – 1023-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type) от 512 до 1023 байт включительно (за исключением битов кадров, но включая байты FCS).
rxHCPkt1024to1518Octets	Счетчик принятых 1024 – 1518-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type) от 1024 до 1518 байт включительно (за исключением битов кадров, но включая байты FCS).
rxHCPkt1519to1522Octets	Счетчик принятых допустимых 1519 – 1522-байтовых кадров VLAN. Увеличивается с каждым допустимым принятым кадром VLAN (исключая FCS, Symbol, ошибка Truncated), от 1519 до 1522 байт включительно (за исключением битов кадров, но включая байты FCS). Подсчитываются как одиночные, так и дважды тегированные кадры.

rxHCPkt1519to2047Octets	Счетчик принятых 1519 – 2047-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type) от 1519 до 2047 байт включительно (за исключением битов кадров, но включая байты FCS).
rxHCPkt2048to4095Octets	Счетчик принятых 2048 – 4095-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type) от 2048 до 4095 байт включительно (за исключением битов кадров, но включая байты FCS).
rxHCPkt4096to9216Octets	Счетчик принятых 4096 – 9216-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 4096 до 9216 байт включительно (за исключением битов кадров, но включая байты FCS).
rxHCPkt9217to16383Octets	Счетчик принятых 9217 – 16383-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type) от 9217 до 16383 байт включительно (за исключением битов кадров, но включая байты FCS).
txHCPkt64Octets	Счетчик переданных 64-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type) до 64 байт включительно (за исключением битов кадров, но включая байты FCS).
txHCPkt65to127Octets	Счетчик переданных 65 – 127-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type) от 65 до 127 байт включительно (за исключением битов кадров, но включая байты FCS).
txHCPkt128to255Octets	Счетчик переданных 128 – 255-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type) от 128 до 255 байт включительно (за исключением битов кадров, но включая байты FCS).
txHCPkt256to511Octets	Счетчик переданных 256 – 511-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type) от 256 до 511 байт включительно (за исключением битов кадров, но включая байты FCS).
txHCPkt512to1023Octets	Счетчик переданных 512 – 1023-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type) от 512 до 1023 байт включительно (за исключением битов кадров, но включая байты FCS).

txHCPkt1024to1518Octets	Счетчик переданных 1024 – 1518-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type) от 1024 до 1518 байт включительно (за исключением битов кадров, но включая байты FCS).
txHCPkt1519to2047Octets	Счетчик переданных 1519 – 2047-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 1519 до 2047 байт включительно (за исключением битов кадров, но включая байты FCS).
txHCPkt2048to4095Octets	Счетчик переданных 2048 – 4095-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type) от 2048 до 4095 байт включительно (за исключением битов кадров, но включая байты FCS).
txHCPkt4096to9216Octets	Счетчик переданных 4096 – 9216-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type) от 4096 до 9216 байт включительно (за исключением битов кадров, но включая байты FCS).
txHCPkt9217to16383Octets	Счетчик переданных 9217 – 16383-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type) от 9217 до 16383 байт включительно (за исключением битов кадров, но включая байты FCS).
rxCRCAlignErrors	Счетчик принятых кадров с ошибкой выравнивания. Увеличивается с каждым принятым пакетом от 64 до max-rcv-frame-size (или max-rcv-frame-size+4 для тегированных кадров) октетов в длину (за исключением битов кадров и включая октеты FCS), но содержащим либо поврежденный FCS с целым числом октетов (ошибка FCS), либо поврежденный FCS с нецелым числом октетов (Ошибка выравнивания).
rxUndersizedPkts	Счетчик принятых кадров неполного размера. Увеличивается с каждым принятым пакетом меньше 64 байт в длину (за исключением битов кадров и включая октеты FCS), но в остальном сформированным верно (содержащим допустимый FCS).
rxOversizedPkts	Счетчик принятых кадров слишком большого размера. Увеличивается с каждым принятым пакетом более 1518 байт в длину (за исключением битов кадров и включая октеты FCS), но в остальном сформированным верно (содержащим допустимый FCS).

rxFragmentPkts	Счетчик принятых фрагментов. Увеличивается с каждым принятым пакетом меньше 64 байт в длину (за исключением битов кадров и включая октеты FCS), но содержащим либо поврежденный FCS с целым числом октетов (ошибка FCS), либо поврежденный FCS с нецелым числом октетов (Ошибка выравнивания).
rxJabbers	Счетчик принятых кадров Jabber. Увеличивается с каждым принятым пакетом более 1518 байт в длину (за исключением битов кадров и включая октеты FCS), но содержащим либо поврежденный FCS с целым числом октетов (ошибка FCS), либо поврежденный FCS с нецелым числом октетов (Ошибка выравнивания).
rxSymbolErrors	Счетчик принятых кадров с ошибкой кода. Увеличивается с каждым принятым кадром, содержащим недопустимый символ данных, но допустимый носитель.
rxBufferFullDropPkts	Счетчик принятых проигнорированных пакетов. Увеличивается с каждым пакетом, проигнорированным по причине заполненного входного буфера или обратного давления (back pressure).
rxACLDropPkts	Счетчик принятых пакетов ACL Drop. Возрастает с каждым пакетом, отброшенным по правилам ACL.
rxMulticastDropPkts	Счетчик принятых пакетов Multicast Drop. Возрастает с каждым отброшенным пакетом multicast (L2+L3).
rxVLANIngressCheckDropPkts	Счетчик принятых пакетов VLAN Drop. Возрастает с каждым пакетом, отброшенным при проверке по VLAN на входе (VLAN ingress).
rxIpv6DropPkts	Счетчик принятых пакетов IPv6 L3 Drop. Возрастает с каждым пакетом, отправленным на интерфейс L3 и проигнорированным по следующим причинам: буфер RX превышает установленное ограничение или GBP заполнен.
rxSTPDropPkts	Счетчик принятых пакетов STP Drop. Возрастает с каждым пакетом, отброшенным по причине того, что статус Spanning Tree State входного порта не находится в состоянии перенаправления.
rxStormAndTableDropPkts	Счетчик принятых пакетов Policy Discard. Возрастает с каждым пакетом, отброшенным благодаря политике получения: действие storm control, действие FDB и т.д.
rxMTUDropPkts	Счетчик принятых кадров MTU Check Error. Возрастает с принятым каждым кадром, размер которого превышает max-rcv-frame-size и который содержит корректный или некорректный FCS. **Примечание**: с тегированием Single VLAN усечение выполняется при max-rcv-frame-size +4; с тегированием double VLAN усечение происходит при max-rcv-frame-size +8.
txCollisions	Счетчик общего числа коллизий при передаче. Возрастает с общим числом коллизий, возникших во время передачи.

ifInErrors	Счетчик принятых пакетов с ошибкой. Возрастает при приеме пакетов, содержащих ошибки, не допускающие их дальшейшую передачу протоколу на уровень выше. Счетчик представляет собой сумму dot3StatsAlignmentErrors, dot3StatsFCSErrors, dot3StatsFrameTooLongs, dot3StatsInternalMacReceiveErrors, dot3StatsSymbolErrors, undersize, fragment, oversize, and jabber error.
ifOutErrors	Счетчик пакетов, переданных с ошибкой. Возрастает при попытке передачи пакетов, содержащих ошибки, не допускающих их дальнейшую передачу. Счетчик является суммой dot3StatsSQETestErrors, dot3StatsLateCollisions, dot3StatsExcessiveCollisions, dot3StatsInternalMacTransmitErrors и dot3StatsCarrierSenseErrors.
ifInDiscards	Счетчик отброшенных принятых пакетов. Возрастает при приеме пакетов, которые в дальшейшем отбрасываются по какой-либо причине. Например, MTU drop, Buffer Full Drop, ACL Drop, Multicast Drop, VLAN Ingress Drop, Invalid IPv6, STP Drop, Storm and FDB Discard и т.д.
ifOutDiscards	Счетчик отброшенных переданных пакетов. Возрастает при передаче пакетов, отброшенных в дальнейшем по какой-либо причине. Например, excessive transit delay discards, HOL drop, STP drop, MTU drop, VLAN drop и т.д.
ifInUnknownProtos	Счетчик полученных, но отброшенных пакетов с неизвестным или не поддерживаемым протоколом. Возрастает с каждым принятым пакетом, который был отброшен из-за неизвестного или не поддерживаемого протокола.
txDelayExceededDiscards	Счетчик просроченных переданных пакетов. Возрастает при передаче пакетов, которые были отброшены из-за превышения времени передачи.
txCRC	Счетчик переданных пакетов с ошибкой FCS. Возрастает с каждым переданным пакетом, не прошедшим проверку FCS.
txSTPDropPkts	Счетчик переданных пакетов STP Drop. Возрастает с каждым пакетом, отброшенным по причине того, что статус Spanning Tree State выходного порта не находится в состоянии перенаправления.
txHOLDropPkts	Счетчик переданных пакетов HOL Drop. Возрастает с каждым пакетом, отброшенным из-за блокировки Head Of Line.
txCoS0DropPkts	Счетчик переданных пакетов COS 0 Drop. Возрастает с каждым пакетом, отброшенным из-за блокировки Head of Line для выходного порта COS 0.
txCoS1DropPkts	Счетчик переданных пакетов COS 1 Drop. Возрастает с каждым пакетом, отброшенным из-за блокировки Head of Line для выходного порта COS 1.

txCoS2DropPkts	Счетчик переданных пакетов COS 2 Drop. Возрастает с каждым пакетом, отброшенным из-за блокировки Head of Line для выходного порта COS 2.
txCoS3DropPkts	Счетчик переданных пакетов COS 3 Drop. Возрастает с каждым пакетом, отброшенным из-за блокировки Head of Line для выходного порта COS 3.
txCoS4DropPkts	Счетчик переданных пакетов COS 4 Drop. Возрастает с каждым пакетом, отброшенным из-за блокировки Head of Line для выходного порта COS 4.
txCoS5DropPkts	Счетчик переданных пакетов COS 5 Drop. Возрастает с каждым пакетом, отброшенным из-за блокировки Head of Line для выходного порта COS 5.
txCoS6DropPkts	Счетчик переданных пакетов COS 6 Drop. Возрастает с каждым пакетом, отброшенным из-за блокировки Head of Line для выходного порта COS 6.
txCoS7DropPkts	Счетчик переданных пакетов COS 7 Drop. Возрастает с каждым пакетом, отброшенным из-за блокировки Head of Line для выходного порта COS 7.
dot3StatsAlignmentErrors	Счетчик принятых кадров Alignment Error. Возрастает с каждым принятым кадром с нецелым числом октетов в длину и не прошедшим проверку FCS. **Примечание:** Подсчет кадров dot3StatsAlignmentErrors зависит от ASIC.
dot3StatsFCSErrors	Счетчик принятых кадров FCS Error. Возрастает с каждым принятым кадром с целым числом октетов в длину, но не прошедшим проверку FCS. **Примечание:** Подсчет кадров dot3StatsFCSErrors зависит от ASIC.
dot3StatsSingleColFrames	Счетчик переданных кадров с одиночной коллизией. Доступен только для режима 10/100. Возрастает с каждым переданным кадром, испытавшим одну коллизию во время передачи.
dot3StatsMultiColFrames	Счетчик переданных кадров многочисленных коллизий. Доступен только в режиме 10/100. Возрастает с каждым успешно переданным кадром, испытавшим больше одной коллизии во время передачи.
dot3StatsSQETestErrors	Счетчик SQET Test Error. Возрастает с каждым сообщением SQE TEST ERROR, сгенерированным подуровнем PLS для отдельного интерфейса. Сообщение SQE TEST ERROR указано в разделе 7.2.2.2.4 ANSI/IEEE 802.3-1985 и его генерирование описано в разделе 7.2.4.6 того же документа. **Примечание**: Данный счетчик не увеличивается при скоростях свыше 10 Мб/с или в режиме полного дуплекса.

dot3StatsDeferredTransmissions	Счетчик одиночных отложенных при передаче кадров. Доступен только в режиме 10/100. Возрастает с каждым переданным кадром, который был отложен при первой попытке передачи и в дальнейшем не подвергся коллизии во время последующей передачи.
dot3StatsLateCollisions	Счетчик кадров поздней коллизии. Доступен только в режиме 10/100. Увеличивается с каждым переданным кадром с поздней коллизией во время попытки передачи.
dot3StatsExcessiveCollisions	Счетчик переданных кадров с избытком коллизий. Доступен только в режиме 10/100. Увеличивается с каждым кадром, передача которого не состоялась из-за избытка коллизий.
dot3StatsInternalMacTransmitErrors	Счетчик переданных кадров с внутренней ошибкой MAC. Возрастает с каждым кадром, передача которого не состоялась из-за ошибки передачи внутреннего подуровня MAC. Кадр учитывается, только если он не был учтен ни одним из следующих счетчиков: dot3StatsLateCollisions, dot3StatsExcessiveCollisions и dot3StatsCarrierSenseErrors.
dot3StatsCarrierSenseErrors	Счетчик False Carrier. Возрастает каждый раз, когда условие контроля несущей потеряно или никогда не подтверждалось при попытке передачи кадра. **Примечание:** Подсчет кадров dot3StatsCarrierSenseErrors зависит от ASIC.
dot3StatsFrameTooLongs	Счетчик принятых кадров слишком большой длины. Возрастает с каждым принятым кадром, превышающим размер max-rcv-frame-size.
dot3StatsInternalMacReceiveErrors	Счетчик Internal MAC Error. Возрастает с каждым кадром, не принятым из-за получения ошибки внутренним подуровнем MAC. Кадр подсчитывается только в том случае, если он не учтен соответствующим экземпляром любого из параметров dot3StatsFrameTooLongs, dot3StatsAlignmentErrors или dot3StatsFCSErrors.

30.6 show interfaces

Данная команда используется для отображения информации об интерфейсе.

show interfaces [*INTERFACE-ID* **[, | -]]**

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейсы, которые необходимо отобразить.

,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если параметры не указаны, будут отображены данные для всех интерфейсов.

Пример

В данном примере показано, как отобразить информацию об интерфейсе VLAN 1.

```
Switch#show interfaces vlan1

Vlan1 is enabled, Link status is down
  Interface type: VLAN
  MAC address: F0-7D-68-12-10-01



Switch#
```

В данном примере показано, как включить отображение информации об интерфейсе для Ethernet 1/0/1.

```
Switch#show interfaces eth1/0/1

Eth1/0/1 is enabled, link status is up
  Interface type: 1000BASE-T
  Interface description:
  MAC Address: 00-01-02-03-04-01
  Auto-duplex, auto-speed, auto-mdix
  Send flow-control: off, receive flow-control: off
  Send flow-control oper: off, receive flow-control oper: off
  Full-duplex, 1Gb/s
  Maximum transmit unit: 1536 bytes
  Rx rate: 0 bytes/sec, TX rate: 0 bytes/sec
  RX bytes: 116316, TX bytes: 132495
  RX rate: 0 packets/sec, TX rate: 0 packets/sec
  RX packets: 1213, TX packets: 365
  RX multicast: 774, RX broadcast: 439
  RX CRC error: 0, RX undersize: 0
  RX oversize: 0, RX fragment: 0
  RX jabber: 0, RX dropped Pkts: 1212
  RX MTU exceeded: 0
  TX CRC error: 0, TX excessive deferral: 0
  TX single collision: 0, TX excessive collision: 0
  TX late collision: 0, TX collision:0

Switch#
```

30.7 show interfaces counters

Данная команда используется для отображения счетчиков на определенных интерфейсах.

show interfaces [*INTERFACE-ID* **[, | -]] counters [errors]**

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейсы, которые необходимо отобразить. Если интерфейс не указан, будут отображаться счетчики для всех интерфейсов. Параметр применим для физических портов.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
errors	(Опционально.) Укажите для отображения счетчика ошибок.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для отображения статистики счетчиков порта коммутатора.

Пример

В данном примере показано, как включить отображение счетчиков для интерфейсов Ethernet 1/0/1-8.

```
Switch# show interfaces eth1/0/1-8 counters

Port          InOctets /            InMcastPkts /
              InUcastPkts           InBcastPkts
------------- --------------------- ---------------------
eth1/0/1      1834520               629
              9234                  338
eth1/0/2      0                     0
              0                     0
eth1/0/3      0                     0
              0                     0
eth1/0/4      0                     0
              0                     0
eth1/0/5      0                     0
              0                     0
eth1/0/6      0                     0
              0                     0
eth1/0/7      0                     0
              0                     0
eth1/0/8      0                     0
              0                     0

Port          OutOctets /           OutMcastPkts /
              OutUcastPkts          OutBcastPkts
------------- --------------------- ---------------------
```

```
eth1/0/1      5387265               0
              9381                  0
eth1/0/2      0                     0
              0                     0
eth1/0/3      0                     0
              0                     0
eth1/0/4      0                     0
              0                     0
eth1/0/5      0                     0
              0                     0
eth1/0/6      0                     0
              0                     0
eth1/0/7      0                     0
              0                     0
eth1/0/8      0                     0
              0                     0

Total Entries:8

Switch#
```

В примере ниже показано, как включить отображение счетчиков ошибок на портах коммутатора.

```
Switch#show interfaces eth1/0/1 counters errors

Port            Align-Err /           Fcs-Err /
                Rcv-Err /             Undersize /
                Xmit-Err              OutDiscard
--------------- --------------------- ----------------------
eth1/0/1        0                     0
                0                     0
                0                     0

Port            Single-Col /          Excess-Col /
                Multi-Col /           Carri-Sen /
                Late-Col              Runts
--------------- --------------------- ----------------------
eth1/0/1        0                     0
                0                     0
                0                     0

Port            Giants /              DeferredTx /
                Symbol-Err /          IntMacTx /
                SQETest-Err           IntMacRx
--------------- --------------------- ----------------------
eth1/0/1        0                     0
                0                     0
                0                     0

Total Entries:1


Switch#
```

Отображаемые параметры

Align-Err	Относится к строке «dot3StatsAlignmentErrors» в разделе «Отображаемые параметры» команды **show counters**.
Rcv-Err	Относится к строке «ifInErrors» в разделе «Отображаемые параметры» команды **show counters**.
Xmit-Err	Относится к строке «ifOutErrors» в разделе «Отображаемые параметры» команды **show counters**.
Fcs-Err	Относится к строке «dot3StatsFCSErrors» в разделе «Отображаемые параметры» команды **show counters**.
UnderSize	Относится к строке «rxUndersizedPkts» в разделе «Отображаемые параметры» команды **show counters**.
OutDiscard	Относится к строке «ifOutDiscards» в разделе «Отображаемые параметры» команды **show counters.**
Single-Col	Относится к строке «dot3StatsSingleColFrames» в разделе «Отображаемые параметры» команды **show counters.**
Multi-Col	Относится к строке «dot3StatsMultiColFrames» в разделе «Отображаемые параметры» команды **show counters.**
Late-Col	Относится к строке «dot3StatsLateCollisions» в разделе «Отображаемые параметры» команды **show counters.**
Excess-Col	Относится к строке «dot3StatsExcessiveCollisions» в разделе «Отображаемые параметры» команды **show counters.**
Carri-Sen	Относится к строке «dot3StatsCarrierSenseErrors» в разделе «Отображаемые параметры» команды **show counters**.
Runts	Увеличивается с каждым пакетом размером менее 64 байт.
Giants	Возрастает с каждым пакетом, размер которого более 1518 байтов в длину.
Symbol-Err	Относится к строке «rxSymbolErrors» в разделе «Отображаемые параметры» команды **show counters**.
SQETst-Err	Относится к строке «dot3StatsSQETestErrors» в разделе «Отображаемые параметры» команды **show counters**.
DeferredTx	Относится к строке «txDelayExceededDiscards» в разделе «Отображаемые параметры» команды **show counters.**
IntMacTx	Относится к строке «dot3StatsInternalMacTransmitErrors» в разделе «Отображаемые параметры» команды **show counters.**
InMacRx	Относится к строке «dot3StatsInternalMacReceiveErrors» в разделе «Отображаемые параметры» команды **show counters**.

30.8 show interfaces status

Данная команда используется для отображения статуса подключения портов коммутатора.

show interfaces [*INTERFACE-ID* **[, | -]] status**

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Команда используется для просмотра состояния подключения портов коммутатора. Если параметр не указан, отображается статус подключения для всех портов коммутатора.

Пример

В данном примере показано, как отобразить статус подключения портов коммутатора.

```
Switch#show interfaces eth1/0/1-8 status

Port          Status        VLAN         Duplex  Speed          Type
------------ ------------ ------------ ------- -------------- ------------
eth1/0/1      connected     1            a-full  a-100          10GBASE-T
eth1/0/2      not-connected 1            auto    auto           10GBASE-T
eth1/0/3      connected     1            a-full  a-100          10GBASE-T
eth1/0/4      not-connected 1            auto    auto           10GBASE-T
eth1/0/5      not-connected 1            auto    auto           10GBASE-T
eth1/0/6      not-connected 1            auto    auto           10GBASE-T
eth1/0/7      not-connected 1            auto    auto           10GBASE-T
eth1/0/8      not-connected 1            auto    auto           10GBASE-T

Total Entries: 8


Switch#
```

30.9 show interfaces utilization

Данная команда используется для отображения информации о загрузке указанных портов коммутатора.

show interfaces [*INTERFACE-ID* **[, | -]] utilization**

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейсы, которые необходимо отобразить. Если параметр не указан, будет отображаться информация о загрузке всех физических портов коммутатора.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
utilization	Укажите для отображения информации о загрузке.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Команда позволяет пользователю отобразить информацию о загрузке портов коммутатора.

Пример

В данном примере показано, как отобразить информацию о загрузке портов коммутатора.

```
Switch#show interfaces eth1/0/1-8 utilization

Port           TX packets/sec    RX packets/sec    Utilization
-------------  ----------------- ----------------- -----------
eth1/0/1       2                 0                 1
eth1/0/2       0                 0                 0
eth1/0/3       0                 2                 1
eth1/0/4       0                 0                 0
eth1/0/5       0                 0                 0
eth1/0/6       0                 0                 0
eth1/0/7       0                 0                 0
eth1/0/8       0                 0                 0

Total Entries:8


Switch#
```

30.10 show interfaces auto-negotiation

Данная команда используется для отображения подробной информации об автосогласовании на физических портах.

show interfaces [*INTERFACE-ID* **[, | -]] auto-negotiation**

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейсы, которые необходимо отобразить. Если параметр не указан, будет отображена информация обо всех физических портах.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
auto-negotiation	Укажите, чтобы отобразить подробную информацию об автосогласовании.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для отображения подробной информации об автосогласовании.

Пример

В данном примере показано, как отобразить информацию об автосогласовании.

```
Switch#show interfaces eth1/0/1-2 auto-negotiation

eth1/0/1
 Auto Negotiation: Enabled

 Remote Signaling: Not detected
 Configure Status: Complete
 Capability Bits: 100M_Full, 1000M_Full, 10G_Full
 Capability Advertised Bits: 100M_Full, 1000M_Full, 10G_Full
 Capability Received Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full
 RemoteFaultAdvertised: Disabled
 RemoteFaultReceived: NoError

eth1/0/2
 Auto Negotiation: Enabled

 Remote Signaling: Not detected
 Configure Status: Configuring
 Capability Bits: 100M_Full, 1000M_Full, 10G_Full
 Capability Advertised Bits: 100M_Full, 1000M_Full, 10G_Full
 Capability Received Bits: -
 RemoteFaultAdvertised: Disabled
 RemoteFaultReceived: NoError


Switch#
```

30.11 show interfaces description

Данная команда используется для отображения описания и состояния интерфейсов.

show interfaces [*INTERFACE-ID* **[, | -]] description**

Параметры

INTERFACE-ID	(Опционально.) Укажите ID интерфейса, который необходимо отобразить. Если параметр не указан, будет отображена информация обо всех интерфейсах.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
description	Укажите для отображения описания и состояния интерфейсов.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Команда используется для отображения описания и состояния интерфейсов.

Пример

В данном примере показано, как отобразить описание и состояние интерфейсов.

```
Switch#show interfaces description

 Interface              Status    Administrative  Description
 ---------------------  --------  --------------  --------------------------------
 eth1/0/1               up        enabled
 eth1/0/2               down      enabled
 eth1/0/3               down      enabled
 eth1/0/4               down      enabled
 eth1/0/5               down      enabled
 eth1/0/6               down      enabled
 eth1/0/7               down      enabled
 eth1/0/8               down      enabled
 eth1/0/9               down      enabled
 eth1/0/10              down      enabled         Physical Port 10
 eth1/0/11              down      enabled
 eth1/0/12              down      enabled
 eth1/0/13              down      enabled
 eth1/0/14              down      enabled
 eth1/0/15              down      enabled
 eth1/0/16              down      enabled
 eth1/0/17              down      enabled
 eth1/0/18              down      enabled
 eth1/0/19              down      enabled
 eth1/0/20              down      enabled
 eth1/0/21              down      enabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

30.12 shutdown

Данная команда используется для отключения интерфейса. Для включения интерфейса воспользуйтесь формой **no** этой команды.

shutdown

no shutdown

Параметры

Нет.

По умолчанию

Опция по умолчанию – **no shutdown**.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и VLAN, а также для портов-участников port-channel.

Команда отключает порт. В отключенном состоянии порт не будет принимать и передавать пакеты. Используйте команду **no shutdown**, чтобы снова включить порт. Если порт отключен, подключение к сети также будет невозможно, и соединения не будет.

Пример

В данном примере показано, как отключить интерфейс Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# shutdown
```

30.13 max-rcv-frame-size

Данная команда используется для настройки максимального размера кадра Ethernet. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

max-rcv-frame-size *BYTES*

no max-rcv-frame-size

Параметры

BYTES	Укажите максимально допустимый размер кадра Ethernet. Диапазон значений: от 64 до 12288 байт.

По умолчанию

По умолчанию используется значение 1536 байт.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.
Кадры слишком большого размера будут отброшены и проверки будут выполняться на входных портах. Используйте данную команду для передачи кадров большого размера или jumbo-фреймов через коммутатор для оптимизации производительности сервер-сервер.

Пример

В данном примере показано, как настроить максимальный размер полученного кадра со значением 6000 на интерфейсе Ethernet 1/0/3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#max-rcv-frame-size 6000
Switch(config-if)#
```

31. Команды Internet Group Management Protocol (IGMP) Snooping

31.1 clear ip igmp snooping statistics

Данная команда используется для удаления статистики IGMP Snooping.

clear ip igmp snooping statistics {all | vlan *VLAN-ID* **| interface** *INTERFACE-ID***}**

Параметры

all	Укажите, чтобы удалить статистику IP IGMP Snooping для всех VLAN и портов.
vlan *VLAN-ID*	Укажите VLAN, для которой необходимо удалить статистику IP IGMP Snooping.
interface *INTERFACE-ID*	Укажите порт, для которого необходимо удалить статистику IP IGMP Snooping.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы удалить статистику IGMP Snooping.

Пример

В данном примере показано, как удалить всю статистику IGMP Snooping.

```
Switch#clear ip igmp snooping statistics all
Switch#
```

31.2 ip igmp snooping

Данная команда используется для включения функции IGMP Snooping на коммутаторе. Для отключения данной функции воспользуйтесь формой **no** этой команды.

ip igmp snooping
no ip igmp snooping

Параметры

Нет.

По умолчанию

По умолчанию функция IGMP Snooping отключена на всех интерфейсах VLAN.

По умолчанию функция IGMP Snooping отключена глобально.

Режим ввода команды

VLAN Configuration Mode.
Global Configuration Mode.

Использование команды

Для того, чтобы предоставить VLAN доступ к IGMP Snooping, необходимо включить данную функцию глобально и для VLAN. Настройки IGMP Snooping и MLD Snooping являются независимыми и могут быть применены для VLAN одновременно.

Пример

В данном примере показано, как отключить IGMP Snooping глобально.

```
Switch# configure terminal
Switch(config)# no ip igmp snooping
Switch(config)#
```

В данном примере показано, как включить функцию IGMP Snooping глобально.

```
Switch#configure terminal
Switch(config)#ip igmp snooping
Switch(config)#
```

В данном примере показано, как отключить IGMP Snooping на VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# no ip igmp snooping
Switch(config-vlan)#
```

31.3 ip igmp snooping fast-leave

Данная команда используется для настройки функции IGMP Snooping Fast Leave на интерфейсе. Для отключения данной функции воспользуйтесь формой **no** этой команды.

ip igmp snooping fast-leave
no ip igmp snooping fast-leave

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Используйте данную команду, чтобы удалить членство IGMP на порту после получения сообщения leave, не применяя механизм обработки сообщений group-specific query (с указанием группы) или group-source-specific query (с указанием источника группы).

Пример

В данном примере показано, как включить функцию IGMP Snooping Fast Leave на VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping fast-leave
Switch(config-vlan)#
```

31.4 ip igmp snooping last-member-query-interval

Данная команда используется для настройки интервала, в течение которого IGMP Snooping Querier отправляет сообщения group-specific query (с указанием группы) или group-source-specific query (с указанием источника группы) / channel-source-specific query (с указанием источника канала). Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip igmp snooping last-member-query-interval *SECONDS*
no ip igmp snooping last-member-query-interval

Параметры

SECONDS	Укажите максимальный интервал между сообщениями group-specific query, включая отправленные в ответ на сообщения leave group. Доступный диапазон значений: от 1 до 25.

По умолчанию

Значение по умолчанию – 1 секунда.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Получив сообщение IGMP leave, IGMP Snooping Querier будет считать, что на VLAN нет локальных участников, если по истечении времени ожидания не будет получено ни одного ответа. Пользователи могут уменьшить данный интервал, чтобы сократить время, которое требуется коммутатору, чтобы обнаружить выход последнего участника из группы.

Пример

В данном примере показано, как настроить значение last member query interval. Указанное значение – 3 секунды.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ip igmp snooping last-member-query-interval 3
Switch(config-vlan)#
```

31.5 ip igmp snooping minimum-version

Данная команда используется для настройки минимальной версии IGMP-узлов, разрешенной на VLAN. Для удаления ограничения воспользуйтесь формой **no** этой команды.

ip igmp snooping minimum-version *NUMBER*
no ip igmp snooping minimum-version

Параметры

NUMBER	Укажите минимальную версию IGMP-узлов: **2:** укажите, чтобы отфильтровать сообщения IGMPv1. **3:** укажите, чтобы отфильтровать сообщения IGMPv1 и IGMPv2.

По умолчанию

По умолчанию ограничения минимальной версии отсутствуют.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Настройки применимы только для фильтрации сообщений IGMP membership report.

Пример

В данном примере показано, как ограничить подключение всех узлов IGMPv1 к VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping minimum-version 2
Switch(config-vlan)#
```

В данном примере показано, как ограничить подключение всех узлов IGMPv1 и IGMPv2 к VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping minimum-version 3
Switch(config-vlan)#
```

В данном примере показано, как удалить ограничения, сконфигурированные на VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#no ip igmp snooping minimum-version
Switch(config-vlan)#
```

31.6 ip igmp snooping mrouter

Данная команда используется для настройки указанного интерфейса/интерфейсов в качестве multicast router-портов, а также для указания интерфейса/интерфейсов, которые не могут быть multicast router-портами. Для удаления интерфейса/интерфейсов из списка router-портов или списка запрещенных router-портов воспользуйтесь формой **no** этой команды.

ip igmp snooping mrouter {interface *INTERFACE-ID* **[, | -] | forbidden interface** *INTERFACE-ID* **[, | -]}**

no ip igmp snooping mrouter {interface *INTERFACE-ID* **[, | -] | forbidden interface** *INTERFACE-ID* **[, | -]}**

Параметры

interface	Укажите статический multicast router-порт.
forbidden interface	Укажите порт, который не может быть multicast router-портом.
INTERFACE-ID	Укажите интерфейс или список интерфейсов. В качестве интерфейса может быть использован физический порт или port-channel.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию multicast router-порты IGMP Snooping отсутствуют.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Multicast router-портом можно назначить физический порт или port-channel. Указанный multicast router-порт должен являться портом-участником сконфигурированной VLAN. Multicast router-порт может быть изучен динамически или сконфигурирован статически. При помощи динамического изучения устройство IGMP Snooping будет изучать пакеты IGMP, PIM или DVMRP, чтобы идентифицировать multicast router-порт.

Пример

В данном примере показано, как добавить статический multicast router-порт IGMP Snooping для VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping mrouter interface eth1/0/4
Switch(config-vlan)#
```

31.7 ip igmp snooping querier

Данная команда используется для указания устройства в качестве IGMP Snooping Querier. Для отключения данной функции воспользуйтесь формой **no** этой команды.

ip igmp snooping querier
no ip igmp snooping querier

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Если система может выполнить роль Querier, устройство будет ожидать пакеты IGMP query, отправленные другими устройствами. При получении сообщения IGMP query устройство с более низким значением IP-адреса становится Querier.

Пример

В данном примере показано, как включить IGMP Snooping Querier на VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping querier
Switch(config-vlan)#
```

31.8 ip igmp snooping query-interval

Данная команда используется для настройки интервала между сообщениями IGMP general query. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip igmp snooping query-interval *SECONDS*
no ip igmp snooping query-interval

Параметры

SECONDS	Укажите интервал между сообщениями IGMP General Query для обозначенного маршрутизатора. Доступный диапазон значений: от 1 до 31731.

По умолчанию

Значение по умолчанию – 125 секунд.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Query Interval – это интервал между сообщениями general query, отправленными Querier. Администратор может настраивать количество IGMP-сообщений, изменяя значение данного интервала: чем больше значение интервала, тем реже будут отправляться сообщения IGMP query.

Пример

В данном примере показано, как настроить интервал IGMP Snooping Query на VLAN 1000. Указанное значение – 300 секунд.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ip igmp snooping query-interval 300
Switch(config-vlan)#
```

31.9 ip igmp snooping query-max-response-time

Данная команда используется, чтобы настроить максимальное значение времени ожидания, анонсированное в сообщениях IGMP snooping query. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip igmp snooping query-max-response-time *SECONDS*
no ip igmp snooping query-max-response-time

Параметры

SECONDS	Укажите максимальное значение времени ожидания, анонсированное в сообщениях IGMP snooping query. Доступный диапазон значений: от 1 до 25 секунд.

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить период времени, в течение которого участник группы может ответить на сообщение IGMP query, прежде чем его принадлежность будет удалена посредством IGMP Snooping.
Интервал group membership life-time рассчитывается следующим образом: query-interval x robustness + max response time.

Пример

В данном примере показано, как настроить максимальное значение времени ожидания на VLAN 1000. Указанное значение – 20 секунд.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ip igmp snooping query-max-response-time 20
Switch(config-vlan)#
```

31.10 ip igmp snooping query-version

Данная команда используется для настройки версии пакетов general query, отправляемых IGMP Snooping Querier. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip igmp snooping query-version *NUMBER*

no ip igmp snooping query-version

Параметры

NUMBER	Укажите версию пакета IGMP general query, отправленного IGMP Snooping Querier. Диапазон значений: от 1 до 3.

По умолчанию

Значение по умолчанию – 3.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Настройки версии пакета query повлияют на выбор Querier. Если выбрана версия 1, IGMP Snooping действует в качестве Querier и не инициирует выбор нового Querier вне зависимости от того, какой пакет IGMP query получен. Если выбрана версия 2 или 3, IGMP Snooping инициирует выбор нового Querier при получении пакета IGMPv2 или IGMPv3, и не инициирует выбор нового Querier при получении пакета IGMPv1.

Пример

В данном примере показано, как настроить версию пакета query на VLAN 1000. Указанная версия – 2.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ip igmp snooping query-version 2
Switch(config-vlan)#
```

31.11 ip igmp snooping report-suppression

Данная команда используется для включения функции Report Suppression. Для отключения данной функции воспользуйтесь формой **no** этой команды.

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Функция Report Suppression работает только для трафика IGMPv1 и IGMPv2. Если функция Report Suppression включена, коммутатор блокирует дублированные отчеты, отправленные узлами. Сообщения IGMP report или IGMP leave одной группы будут блокироваться до тех пор, пока не истечет установленное время. Для одной группы будет передано только одно сообщение IGMP report или IGMP leave, остальные сообщения будут заблокированы.

Пример

В данном примере показано, как включить функцию Report Suppression на VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping report-suppression
Switch(config-vlan)#
```

31.12 ip igmp snooping robustness-variable

Данная команда используется для настройки robustness variable (переменной надежности), используемой в IGMP Snooping. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip igmp snooping robustness-variable *VALUE*
no ip igmp snooping robustness-variable

Параметры

VALUE	Укажите значение robustness variable в диапазоне от 1 до 7.

По умолчанию

Значение по умолчанию – 2.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Robustness variable обеспечивает точную настройку в соответствии с ожидаемой потерей пакетов в VLAN. Значение robustness variable используется для расчета следующих интервалов IGMP-сообщений:

- **Group member interval** – промежуток времени, по истечении которого маршрутизатор считает, что в группе больше нет активных участников. Данный интервал рассчитывается следующим образом: (robustness variable x query interval) + (1 x query response interval).
- **Other querier present interval** – промежуток времени, по истечении которого многоадресный маршрутизатор считает, что маршрутизатор, являющийся Querier, больше не доступен. Данный интервал рассчитывается следующим образом: (robustness variable x query interval) + (0,5 x query response interval).
- **Last member query count** – количество запросов group-specific query (с указанием группы), отправленных маршрутизатором до того, как он предполагает, что в группе нет локальных участников. Robustness variable является значением по умолчанию данного счетчика.

Пользователи могут увеличить данное значение, если для сети требуются более свободные условия.

Пример

В данном примере показано, как настроить robustness variable на интерфейсе VLAN 1000. Указанное значение – 3.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ip igmp snooping robustness-variable 3
Switch(config-vlan)#
```

31.13 ip igmp snooping static-group

Данная команда используется для настройки статической группы IGMP Snooping. Для удаления статической группы воспользуйтесь формой **no** этой команды.

ip igmp snooping static-group *GROUP-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**
no ip igmp snooping static-group *GROUP-ADDRESS* **[interface** *INTERFACE-ID* **[, | -]]**

Параметры

GROUP-ADDRESS	Укажите IP-адрес многоадресной группы.
interface *INTERFACE-ID*	Укажите интерфейс или список интерфейсов. Доступны физические порты или port-channel.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию статическая группа не настроена.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Используйте данную команду, чтобы создать статическую группу IGMP Snooping, если подключенный узел не поддерживает IGMP-протокол.

Пример

В данном примере показано, как добавить запись статической группы для IGMP Snooping.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping static-group 226.1.2.3 interface eth1/0/5
Switch(config-vlan)#
```

31.14 ip igmp snooping suppression-time

Данная команда используется, чтобы настроить время подавления (suppression) дублированных сообщений IGMP report или IGMP leave. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip igmp snooping suppression-time *SECONDS*

no ip igmp snooping suppression-time

Параметры

SECONDS	Укажите время подавления дублированных сообщений IGMP report. Доступный диапазон значений: от 1 до 300.

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Функция Report Suppression подавляет дублированные пакеты IGMP report или IGMP leave, полученные в течение указанного времени. Чем меньше значение времени подавления, тем чаще будут отправляться дублированные IGMP-пакеты.

Пример

В данном примере показано, как настроить время подавления на интерфейсе VLAN 1000. Указанное значение – 125.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ip igmp snooping suppression-time 125
Switch(config-vlan)#
```

31.15 show ip igmp snooping

Данная команда используется для отображения информации об IGMP Snooping на коммутаторе.

show ip igmp snooping [vlan *VLAN-ID***]**

Параметры

vlan *VLAN-ID*	(Опционально.) Укажите VLAN, которую необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить информацию об IGMP Snooping для всех VLAN, на которых включена данная функция.

Пример

В данном примере показано, как отобразить общее состояние IGMP Snooping.

```
Switch# show ip igmp snooping

IGMP snooping global state: Enabled

Switch#
```

В данном примере показано, как отобразить информацию об IGMP Snooping для VLAN 1.

```
Switch#show ip igmp snooping vlan 1

VLAN #1 configuration
    IGMP snooping state             : Disabled
    Minimum version                 : v1
    Fast leave                      : Disabled (port-based)
    Report suppression              : Disabled
    Suppression time                : 10 seconds
    Querier state                   : Disabled
    Query version                   : v3
    Query interval                  : 125 seconds
    Max response time               : 10 seconds
    Robustness value                : 2
    Last member query interval      : 1 seconds

Total Entries: 1

Switch#
```

31.16 show ip igmp snooping groups

Данная команда используется для отображения информации о группе IGMP Snooping, изученной на коммутаторе.

show ip igmp snooping groups [vlan *VLAN-ID* **[, | -] | [***IP-ADDRESS***] [detail]**

Параметры

vlan *VLAN-ID*	(Опционально.) Укажите интерфейс VLAN для отображения. Если VLAN не указана, будет отображена информация о группе IGMP Snooping для всех VLAN с включенной функцией IGMP Snooping.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
IP-ADDRESS	(Опционально.) Укажите IP-адрес группы для отображения. Если IP-адрес не указан, будет отображена информация обо всех группах IGMP.
detail	(Опционально.) Укажите для отображения подробной информации о группе IGMP.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить информацию о группе IGMP Snooping.

Пример

В данном примере показано, как отобразить информацию о группе IGMP Snooping.

```
Switch#show ip igmp snooping groups

Total Group Entries : 1
Total Source Entries: 2

vlan1, 230.1.1.1
Learned on port: 1/0/3,1/0/5

Switch#
```

В данном примере показано, как отобразить информацию о группе IGMP Snooping.

```
Switch#show ip igmp snooping groups detail

Total Group Entries : 1
Total Source Entries: 2

vlan1, 230.1.1.1
Learned on port: 1/0/3,1/0/5
  1/0/3
    version: v2, filter mode: Exclude, uptime: 0DT00H00M05S, expires: 0DT00H04M16S
  1/0/5
    version: v3, filter mode: Include, uptime: 0DT00H00M07S, expires: 0DT00H00M00S
      source 192.168.1.1, uptime: 0DT00H00M07S, expires: 0DT00H04M13S

Switch#
```

31.17 show ip igmp snooping mrouter

Данная команда используется для отображения информации о маршрутизаторе IGMP Snooping, который был изучен и настроен на коммутаторе.

show ip igmp snooping mrouter [vlan *VLAN-ID***]**

Параметры

vlan *VLAN-ID*	(Опционально.) Укажите VLAN, которую необходимо отобразить. Если VLAN не указана, будет отображена информация об IGMP Snooping на всех VLAN.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить интерфейсы динамически изученного или настроенного вручную многоадресного маршрутизатора.
Если параметр не указан, будет отображена информация об IGMP Snooping на всех VLAN.

Пример

В данном примере показано, как отобразить информацию о многоадресном маршрутизаторе IGMP Snooping на VLAN 1.

```
Switch#show ip igmp snooping mrouter vlan 1

VLAN   Ports
-----  ---------------------------
1      eth1/0/7 (static)

Total Entries: 1

Switch#
```

31.18 show ip igmp snooping static-group

Данная команда используется для отображения статически настроенных групп IGMP Snooping на коммутаторе.

show ip igmp snooping static-group [*GROUP-ADDRESS* **| vlan** *VLAN-ID***]**

Параметры

GROUP-ADDRESS	(Опционально.) Укажите IP-адрес группы, которую необходимо отобразить.
vlan *VLAN-ID*	(Опционально.) Укажите VLAN ID, который необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить статически настроенные группы IGMP Snooping на коммутаторе. Если дополнительные параметры не выбраны, будет отображена вся информация.

Пример

В данном примере показано, как отобразить статически настроенные группы IGMP Snooping.

```
Switch#show ip igmp snooping static-group

VLAN ID  Group address    Interface
-------  --------------  ----------------------
1        230.1.1.1       eth1/0/2-1/0/5

Total Entries: 1

Switch#
```

31.19 show ip igmp snooping statistics

Данная команда используется для отображения информации о статистике IGMP Snooping на коммутаторе.

show ip igmp snooping statistics {interface [*INTERFACE-ID* **[, | -]] | vlan [***VLAN-ID* **[, | -]]}**

Параметры

interface	Укажите, чтобы отобразить счетчики статистики интерфейса. Разрешены физические порты и port-channel.
INTERFACE-ID	(Опционально.) Укажите интерфейс, который необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
vlan	Укажите, чтобы отобразить счетчики статистики VLAN.
VLAN-ID	(Опционально.) Укажите VLAN ID, который необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить информацию о статистике IGMP Snooping.

Пример

В данном примере показано, как отобразить информацию о статистике IGMP Snooping.

```
Switch#show ip igmp snooping statistics vlan 1


VLAN 1 Statistics:
  IGMPv1 Rx: Report 0, Query 0
  IGMPv2 Rx: Report 0, Query 0, Leave 0
  IGMPv3 Rx: Report 3, Query 0
  IGMPv1 Tx: Report 0, Query 0
  IGMPv2 Tx: Report 0, Query 0, Leave 0
  IGMPv3 Tx: Report 1, Query 2

Total Entries: 1

Switch#
```

32. Команды IP-MAC-Port Binding (IMPB)

32.1 clear ip ip-mac-port-binding violation

Данная команда используется для удаления заблокированных записей IP-MAC-Port Binding (IMPB).

clear ip ip-mac-port-binding violation {all | interface *INTERFACE-ID* **|** *MAC-ADDRESS***}**

Параметры

all	Укажите для удаления всех неразрешенных записей.
interface *INTERFACE-ID*	Укажите для удаления неразрешенных записей, созданных определенным интерфейсом.
MAC-ADDRESS	Укажите для удаления неразрешенных записей с определенным MAC-адресом.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Команда используется для удаления неразрешенных записей IMPB из базы данных фильтрации.

Пример

В данном примере показано, как удалить заблокированную запись на интерфейсе Ethernet 1/0/4.

```
Switch#clear ip ip-mac-port-binding violation interface eth1/0/4
Switch#
```

32.2 ip ip-mac-port-binding

Данная команда используется для включения управления доступом IMPB для интерфейсов порта. Для отключения функции управления доступом IMPB воспользуйтесь формой **no** этой команды.

ip ip-mac-port-binding [*MODE***]**
no ip ip-mac-port-binding

Параметры

MODE	Укажите режим управления доступом IMPB. • **strict-mode:** укажите для включения режима управления доступом strict. • **loose-mode:** укажите для включения режима управления доступом loose.

	Если режим не задан, используется **strict-mode.**

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.

Если на порту назначен режим управления доступом IMPB **strict-mode**, узел может получить доступ к порту только после того, как узел отправит ARP или IP-пакеты, и эти пакеты пройдут проверку привязки. Чтобы пройти проверку привязки, IP и MAC-адрес источника, VLAN ID и номер порта назначения должны совпадать с любой записью, определенной либо статической записью привязки IP Source Guard, либо изученной динамической записью привязки DHCP Snooping.

Если на порту назначен режим управления доступом IMPB **loose-mode**, узлу будет отказано в доступе к порту после отправки узлом ARP или IP-пакетов, а эти пакеты, отправленные узлом, не пройдут проверку привязки. Чтобы пройти проверку привязки, IP и MAC-адрес источника, VLAN ID и номер порта назначения должны совпадать с любой записью, определенной либо статической записью привязки IP Source Guard, либо изученной динамической записью привязки DHCP Snooping.

Пример

В данном примере показано, как включить управление доступом IMPB на интерфейсе Ethernet 1/0/10.

```
Switch#configure terminal
Switch(config)#interface eth1/0/10
Switch(config-if)#ip ip-mac-port-binding strict
Switch(config-if)#
```

32.3 show ip ip-mac-port-binding

Данная команда используется для отображения настроек IMPB или записей, заблокированных с помощью управления доступом IMPB.

show ip ip-mac-port-binding [interface *INTERFACE-ID* **[, | -]] [violation]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите для отображения определенного интерфейса.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

violation	(Опционально.) Укажите для отображения заблокированной записи.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте команду **show ip ip-mac-port-binding** для отображения настроек IMPB. Используйте команду **show ip ip-mac-port-binding violation** для отображения записей, заблокированных из-за нарушения проверки IMPB.

Пример

В данном примере показано, как включить отображение всех заблокированных записей управления доступом IMPB.

```
Switch#show ip ip-mac-port-binding violation
Port            VLAN MAC Address
--------------- ---- -----------------
eth1/0/3        1    01-00-0C-CC-CC-CC
eth1/0/3        1    01-80-C2-00-00-00
eth1/0/4        1    01-00-0C-CC-CC-CD
eth1/0/4        1    01-80-C2-00-00-01

Total Entries: 4

Switch#
```

В данном примере показано, как включить отображение настроек IMPB для всех портов.

```
Switch#show ip ip-mac-port-binding

Port           Mode
---------- ------------
eth1/0/1       Strict
eth1/0/2       Strict
eth1/0/3       Loose
eth1/0/4       Loose

Total Entries: 4

Switch#
```

32.4 snmp-server enable traps ip-mac-port-binding

Данная команда используется, чтобы включить уведомления SNMP для привязки IP-MAC-Port Binding. Для отключения уведомлений SNMP воспользуйтесь формой **no** этой команды.

snmp-server enable traps ip-mac-port-binding

no snmp-server enable traps ip-mac-port-binding

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте эту команду для включения или отключения отправки SNMP-уведомлений для таких событий. При включении данной функции коммутатор будет отправлять trap-сообщения при нарушениях безопасности, если будет получен некорректный пакет.

Пример

В данном примере показано, как включить отправку trap-сообщений для IP-MAC-Port Binding.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps ip-mac-port-binding
Switch(config)#
```

33. Команды IP Multicast (IPMC)

33.1 show ip mroute forwarding-cache

Данная команда позволяет отобразить содержимое базы данных кэша перенаправления IP multicast routing.

show ip mroute forwarding-cache [group-addr *GROUP-ADDRESS* **[source-addr** *SOURCE-ADDRESS***]]**

Параметры

group-addr *GROUP-ADDRESS*	(Опционально.) Укажите IP-адрес группы.
source-addr *SOURCE-ADDRESS*	(Опционально.) Укажите IP-адрес multicast-источника.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Кэш перенаправления IP multicast представляет собой сводную таблицу на основе таблицы маршрутизации IP multicast, таблицы участников группы IGMP snooping и multicast router-портов.

Пример

В данном примере показано, как отобразить содержимое кэша перенаправления IP multicast routing.

```
Switch#show ip mroute forwarding-cache
(10.1.1.1, 239.0.0.0) VLAN0060
  Outgoing interface list: eth1/0/1, port-channel2

(*,225.0.0.0) VLAN0070
  Outgoing interface list: eth1/0/1-1/0/2

Total entries: 2

Switch#
```

Отображение параметров

239.0.0.0	Адрес группы.
10.1.1.1	Адрес источника.
*****	Подстановочный (wildcard) адрес источника.
VLAN0060	Интерфейс, на который поступают данные многоадресной рассылки.

Outgoing interface list	Список исходящих интерфейсов для многоадресной передачи данных. Содержит интерфейсы коммутации уровня 2.

34. Команды IP Multicast Version 6 (IPMCv6)

34.1 show ipv6 mroute forwarding-cache

Данная команда позволяет отобразить содержимое базы данных кэша перенаправления IPv6 multicast routing.

show ipv6 mroute forwarding-cache [group-addr *GROUP-ADDRESS* **[source-addr** *SOURCE-ADDRESS***]]**

Параметры

group-addr *GROUP-ADDRESS*	(Опционально.) Укажите IPv6-адрес группы.
source-addr *SOURCE-ADDRESS*	(Опционально.) Укажите IPv6-адрес multicast-источника.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Кэш перенаправления IPv6 multicast представляет собой сводную таблицу на основе таблицы маршрутизации IPv6 multicast, таблицы участников группы MLD Snooping и multicast router-портов.

Пример

В данном примере показано, как отобразить содержимое кэша перенаправления IPv6 multicast routing.

```
Switch# show ipv6 mroute forwarding-cache
(2000:60:1:1::10, ff0e::1:1:1) VLAN0060
  Outgoing interface list: eth1/0/1, port-channel2

(2000:60:1:1::10, ff0e::1:1:2) VLAN0060
  Outgoing interface list: eth1/0/1, eth1/0/3

Total entries: 2

Switch#
```

Отображение параметров

FF0E::1:1:1	Адрес группы.
2000:60:1:1::10	Адрес источника.
VLAN0060	Интерфейс, на который поступают данные многоадресной рассылки.

Outgoing interface list	Список исходящих интерфейсов для многоадресной передачи данных. Содержит интерфейсы коммутации уровня 2.

35. Команды IP Source Guard

35.1 ip verify source vlan dhcp-snooping

Данная команда используется для включения на порту функции защиты IP-адреса – IP Source Guard. Для отключения IP Source Guard воспользуйтесь формой **no** этой команды.

ip verify source vlan dhcp-snooping [ip-mac]

no ip verify source vlan dhcp-snooping [ip-mac]

Параметры

ip-mac	(Опционально.) Укажите для проверки IP- и MAC-адреса получаемых IP-пакетов.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и port-channel.

Используйте команду для включения IP Source Guard на необходимом порту.

При включении на порту IP Source Guard IP-пакеты, приходящие на порт, будут проверяться списком управления доступом (ACL). Порт ACL – аппаратный механизм, записи которого могут быть настроены вручную либо получены с помощью таблицы DHCP. Пакет, не прошедший проверку, будет отброшен.

Существует два типа проверки:

Если **ip-mac** не указан, проверка основана только на IP-адресе источника и VLAN.

Если **ip-mac** указан, проверка основана на MAC-адресе источника, VLAN и IP-адресе источника.

Пример

В данном примере показано, как включить IP Source Guard для интерфейса Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip verify source vlan dhcp-snooping
Switch(config-if)#
```

35.2 ip source binding

Данная команда используется для создания статической записи для IP Source Guard. Для удаления статической записи привязки воспользуйтесь формой **no** этой команды.

ip source binding *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**

no ip source binding *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**

Параметры

MAC-ADDRESS	Укажите MAC-адрес для привязки IP-to-MAC.
vlan *VLAN-ID*	Укажите VLAN, которой принадлежит проверенный узел.
IP-ADRESS	Укажите IP-адрес для привязки IP-to-MAC.
interface *INTERFACE-ID*	Укажите порт, к которому подключен проверенный узел. Доступны только интерфейсы физического порта и port-channel.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.

Используйте данную команду для создания или удаления статической привязки, используемой для проверки IP Source Guard. Указанные параметры команды должны в точности совпадать с настроенными параметрами для удаления.

Если MAC-адрес и VLAN настраиваемой привязки уже есть, существующая привязка будет обновлена.

Пример

В данном примере показано, как настроить привязку IP Source Guard с IP-адресом 10.1.1.1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 на интерфейсе Ethernet 1/0/10.

```
Switch#configure terminal
Switch(config)#ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface eth1/0/10
Switch(config)#
```

В данном примере показано, как удалить привязку IP Source Guard с IP-адресом 10.1.1.1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 на интерфейсе Ethernet 1/0/10.

```
Switch#configure terminal
Switch(config)#no ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface eth1/0/10
Switch(config)#
```

35.3 show ip source binding

Данная команда используется для отображения привязки IP Source Guard.

show ip source binding [*IP-ADDRESS***] [***MAC-ADDRESS***] [dhcp-snooping | static] [vlan** *VLAN-ID***]**

[interface *INTERFACE-ID* **[, | -]]**

Параметры

IP-ADDRESS	(Опционально.) Укажите для отображения привязки IP Source Guard на основе IP-адреса.
MAC-ADDRESS	(Опционально.) Укажите для отображения привязки IP Source Guard на основе MAC-адреса.
dhcp-snooping	(Опционально.) Укажите для отображения привязки IP Source, изученной при помощи DHCP Snooping.
static	(Опционально.) Укажите для отображения привязки IP Source Guard, настроенной вручную.
vlan *VLAN-ID*	(Опционально.) Укажите для отображения привязки IP Source Guard на основе VLAN.
interface *INTERFACE-ID*	(Опционально.) Укажите для отображения привязки IP Source Guard на основе порта.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Записи привязки IP Source Guard либо настраиваются вручную, либо изучаются автоматически с помощью DHCP Snooping для защиты IP-трафика.

Пример

В данном примере показано, как отобразить все записи привязки привязки IP Source Guard.

```
Switch#show ip source binding

MAC Address       IP Address      Lease(sec)  Type         VLAN Interface
----------------- --------------- ---------- ------------- ---- ---------
00-01-01-01-01-10 10.1.1.11       infinite   static        1    eth1/0/3
00-01-02-03-04-05 10.1.1.1        infinite   static        2    eth1/0/10

Total Entries: 2

Switch#
```

Отображаемые параметры

MAC Address	MAC-адрес клиента.
IP Address	IP-адрес клиента, назначенный DHCP-сервером или настроенный пользователем.
Lease (sec)	Время аренды IP-адреса.
Type	Тип привязки. Статическая привязка настраивается вручную. Динамическая привязка изучается с помощью DHCP Snooping.
VLAN	Номер VLAN, где находится интерфейс клиента.
Interface	Интерфейс, подключаемый к узлу DHCP-клиента.

35.4 show ip verify source

Данная команда используется для отображения записи списка управления доступом (ACL) аппаратного порта на определенном интерфейсе.

show ip verify source [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите порт или диапазон портов для отображения.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для отображения записей в аппаратной таблице ACL.

Пример

В данном примере показано, как отобразить запись, если на VLAN 100 – VLAN 110 включен DHCP Snooping, на интерфейсе активирован режим IP Source Filter Mode, настроенный как IP, а текущая привязка произведена на основе IP-адреса 10.1.1.1 на VLAN 100.

```
Switch#show ip verify source interface eth1/0/3

Interface       Filter-type Filter-mode IP address      MAC address       VLAN
---------       ----------- ----------- --------------- ----------------- ----
eth1/0/3        ip          active      10.1.1.1        -                 100
eth1/0/3        ip          active      deny-all        -                 101-120

Total Entries: 2

Switch#
```

В данном примере показано, как отобразить запись, если интерфейс в режиме IP Source Filter Mode настроен как IP MAC, и существует привязка IP-адреса 10.1.1.10 к MAC-адресу 00-01-01-01-01-01 в VLAN 100, а также IP-адреса 10.1.1.11 к MAC-адресу 00-01-01-01-01-10 в VLAN 101.

```
Switch#show ip verify source interface eth1/0/3

Interface       Filter-type Filter-mode IP address      MAC address       VLAN
---------       ----------- ----------- --------------- ----------------- ----
eth1/0/3        ip-mac      active      10.1.1.10       00-01-01-01-01-01 100
eth1/0/3        ip-mac      active      10.1.1.11       00-01-01-01-01-10 101
eth1/0/3        ip-mac      active      deny-all                -         102-120

Total Entries: 3

Switch#
```

Отображаемые параметры

Interface	Интерфейс, на котором включен IP Inspection.
Filter-type	Тип действующего IP Source Guard. **ip:** для авторизации IP-пакетов используется только IP-адрес. **ip-mac:** для авторизации IP-пакетов используется IP и MAC-адрес.
Filter-Mode	**active:** активная проверка записей IP Source. **inactive-trust-port:** включить DHCP Snooping для доверенных портов без активной проверки записей IP Source. **inactive-no-snooping-vlan:** не настроено DHCP Snooping в VLAN, нет активной проверки записей IP Source.
IP address	IP-адрес клиента, назначенный DHCP-сервером или настроенный пользователем.

MAC address	MAC-адрес клиента.
VLAN	Номер VLAN интерфейса клиента.

36. Команды IP Utility

36.1 ping

Данная команда используется для диагностики базового сетевого соединения.

ping {[ip] *IP-ADDRESS* **| [ipv6]** *IPV6-ADDRESS* **|** *HOST-NAME***} [count** *TIMES***] [timeout** *SECONDS***]**

[source {*IP-ADDRESS* **|** *IPV6-ADDRESS***}]**

Параметры

ip	(Опционально.) Укажите, чтобы использовать IPv4-адрес назначения (destination).
IP-ADDRESS	Укажите IPv4-адрес узла назначения.
ipv6	(Опционально.) Укажите, чтобы использовать IPv6-адрес назначения.
IPV6-ADDRESS	Укажите IPv6-адрес системы, который необходимо обнаружить.
HOST-NAME	Укажите имя узла системы для обнаружения.
count *TIMES*	(Опционально.) Укажите, чтобы завершить процесс после отправки указанного количества пакетов echo request.
timeout *SECONDS*	(Опционально.) Укажите время ожидания ответа в секундах.
source {*IP-ADDRESS* **|** *IPV6-ADDRESS***}**	(Опционально.) Укажите IP-адрес источника (source), используемый для пакетов команды **ping**. Указанный IP-адрес должен быть одним из IP-адресов, сконфигурированных для коммутатора. У IP-адреса назначения и IP-адреса источника должен быть один тип – IPv4 или IPv6.

По умолчанию

Параметр **count** отключен. Проверка ping будет продолжаться до тех пор, пока пользователь не завершит процесс.
Значение **timeout** – 1 секунда.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы проверить доступность, надежность и задержку маршрута к узлу назначения.

Чтобы прервать ping принудительно, используйте сочетание клавиш CTRL+C.

Пример

В данном примере показано, как протестировать узел с IP-адресом 211.21.180.1. Значение параметра **count** – 4.

```
Switch# ping 211.21.180.1 count 4

Reply from 211.21.180.1, time=10ms
Reply from 211.21.180.1, time<10ms
Reply from 211.21.180.1, time<10ms
Reply from 211.21.180.1, time<10ms

 Ping Statistics for 211.21.180.1
 Packets: Sent =4, Received =4, Lost =0


Switch#
```

В данном примере показано, как проверить узел с IPv6-адресом 2001:238:f8a:77:7c10:41c0:6ddd:ecab.

```
Switch# ping 2001:238:f8a:77:7c10:41c0:6ddd:ecab

Reply from 2001:238:f8a:77:7c10:41c0:6ddd:ecab , bytes=100, time<10 ms
Reply from 2001:238:f8a:77:7c10:41c0:6ddd:ecab , bytes=100, time<10 ms
Reply from 2001:238:f8a:77:7c10:41c0:6ddd:ecab , bytes=100, time<10 ms
Reply from 2001:238:f8a:77:7c10:41c0:6ddd:ecab , bytes=100, time<10 ms

 Ping Statistics for 2001:238:f8a:77:7c10:41c0:6ddd:ecab
 Packets: Sent =4, Received =4, Lost =0

Switch#
```

36.2 ping access-class

Данная команда используется для указания списка доступа, который ограничит доступ для ping. Для удаления проверки при помощи списка доступа воспользуйтесь формой **no** этой команды.

ping access-class *IP-ACL*
no ping access-class *IP-ACL*

Параметры

IP-ACL	Укажите стандартный список доступа IP. Поле адреса источника (source) разрешающей или запрещающей записи определяет, действителен узел, или нет. Чтобы разрешить доступ для ping, укажите поле адреса источника, а в поле адреса назначения списка доступа укажите «any» (при наличии поля).

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы указать список доступа, который ограничит доступ для ping. Для выполнения команды указанный список доступа не обязательно должен существовать.

Пример

В данном примере показано, как создать класс доступа ping, который используется для ограничения Ping только хостом 220.1.1.1 через стандартный список доступа IP.

```
Switch# configure terminal
Switch(config)# ip access-list ping-filter
Switch(config-ip-acl)# permit 220.1.1.1 255.255.255.255
Switch(config-ip-acl)# exit
Switch(config)# ping access-class ping-filter
Switch(config)#
```

37. Команды IPv6 Snooping

37.1 ipv6 snooping policy

Данная команда используется для создания или изменения политики IPv6 Snooping. Команда позволяет войти в режим IPv6 Snooping Configuration Mode. Для удаления политики IPv6 Snooping воспользуйтесь формой **no** этой команды.

ipv6 snooping policy *POLICY-NAME*
no ipv6 snooping policy *POLICY-NAME*

Параметры

POLICY-NAME	Укажите имя политики IPv6 Snooping.

По умолчанию

По умолчанию ни одной политики IPv6 Snooping не создано.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для создания политики IPv6 Snooping. После создания политики IPv6 Snooping используйте команду **ipv6 snooping attach-policy** для применения политики на указанном интерфейсе.

Пример

В данном примере показано, как создать политику IPv6 Snooping с именем policy1.

```
Switch#configure terminal
Switch(config)#ipv6 snooping policy policy1
Switch(config-ipv6-snooping)#
```

37.2 protocol

Данная команда используется для указания того, что адреса должны отслеживаться с помощью DHCPv6 или NDP. При использовании формы **no** данная команда отключит IPv6 Snooping для указанного протокола.

protocol {dhcp | ndp}
no protocol {dhcp | ndp}

Параметры

dhcp	Укажите для отслеживания адресов DHCPv6-пакетов.
ndp	Укажите для отслеживания адресов NDP-пакетов.

По умолчанию

По умолчанию DHCPv6 Snooping и ND Snooping отключены.

Режим ввода команды

IPv6 Snooping Configuration Mode.

Использование команды

Функция Neighbor Discovery (ND) Snooping используется для IPv6-адресов, настроенных вручную или созданных с помощью механизма автоконфигурации Stateless Autoconfiguration. Перед назначением IPv6-адреса узел должен сначала выполнить обнаружение Duplicate Address Detection (DAD), позволяющее определить дублирование адресов узлов локальной сети. ND Snooping обнаруживает сообщения DAD, включающие DAD Neighbor Solicitation (NS) и DAD Neighbor Advertisement (NA), для построения таблицы привязок. NDP-пакет (NS и NA) также используется, чтобы определить, доступен ли узел по-прежнему и можно ли удалить привязку.

DHCPv6 Snooping анализирует DHCPv6-пакеты, отправляемые между DHCPv6-клиентом и сервером во время процедуры назначения адреса. Когда DHCPv6-клиент успешно получает действительный IPv6-адрес, DHCPv6 Snooping создает свою таблицу привязок.

Пример

В данном примере показано, как включить DHCPv6 Snooping.

```
Switch#configure terminal
Switch(config)#ipv6 snooping policy policy1
Switch(config-ipv6-snooping)#protocol dhcp
Switch(config-ipv6-snooping)#
```

37.3 limit address-count

Данная команда используется для ограничения максимального количества привязок IPv6 Snooping. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

limit address-count *MAXIMUM*
no limit address-count

Параметры

MAXIMUM	Укажите максимальное количество привязок IPv6 Snooping. Диапазон значений: от 0 до 511.

По умолчанию

По умолчанию ограничений нет.

Режим ввода команды

IPv6 Snooping Configuration Mode.

Использование команды

Данная команда используется для ограничения количества привязок IPv6 Snooping, для которых применяется политика IPv6 Sooping. Команда помогает ограничить размер таблицы привязок.

Пример

В данном примере показано, как задать максимальное число записей IPv6 Snooping. Указанное значение – 25.

```
Switch#configure terminal
Switch(config)#ipv6 snooping policy policy1
Switch(config-ipv6-snooping)#limit address-count 25
Switch(config-ipv6-snooping)#
```

37.4 ipv6 snooping attach-policy

Данная команда используется для применения политики IPv6 Snooping к указанной VLAN. Для удаления привязки воспользуйтесь формой **no** этой команды.

ipv6 snooping policy attach-policy *POLICY-NAME*
no ipv6 snooping policy attach-policy

Параметры

POLICY-NAME	Укажите имя политики IPv6 Snooping.

По умолчанию

Нет.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

После создания политики IPv6 Snooping Policy используйте данную команду для применения политики к определенной VLAN.

Пример

В данном примере показано, как включить IPv6 Snooping в VLAN 200.

```
Switch# configure terminal
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# limit address-count 100
Switch(config-ipv6-snooping)# exit
Switch(config)# vlan 200
Switch(config-vlan)# ipv6 snooping attach-policy policy1
Switch(config-vlan)#
```

37.5 ipv6 snooping station-move deny

Данная команда используется, чтобы запретить функцию Station Move для привязки IPv6 Snooping. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 snooping station-move deny
no ipv6 snooping station-move deny

Параметры

Нет.

По умолчанию

По умолчанию функция Station Move разрешена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Когда функция Station Move разрешена, динамическая запись привязки Snooping с тем же VLAN ID и MAC-адресом на указанном порту может продвинуться к другому порту, если обнаружены следующие условия:

- Запись привязки DHCPv6 Snooping запускает новый DHCP-процесс на новом интерфейсе;
- Запись привязки ND Snooping запускает новый DAD-процесс на новом интерфейсе.

Пример

В данном примере показано, как запретить функцию Station Move.

```
Switch#configure terminal
Switch(config)#ipv6 snooping station-move deny
Switch(config)#
```

37.6 show ipv6 snooping policy

Данная команда используется для просмотра информации о DHCPv6 Guard.

show ipv6 snooping policy [*POLICY-NAME***]**

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики DHCPv6 Guard, которую необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для просмотра информации о DHCPv6 Guard. Если параметр не указан, будет отображаться информация для всех политик.

Пример

В данном примере показано, как включить отображение информации о DHCPv6 Guard.

```
Switch#show ipv6 snooping policy

Snooping policy: policy1
    Protocol: DHCP
    Limit Address Count: 25
    Target VLAN: 200

Switch#
```

38. Команды IPv6 Source Guard

38.1 ipv6 source binding vlan

Данная команда используется для добавления статической записи в таблицу привязок. Для удаления статической привязки воспользуйтесь формой **no** этой команды.

ipv6 source binding *MAC-ADDRESS* **vlan** *VLAN-ID IPV6-ADDRESS* **interface** *INTERFACE-ID*
no ipv6 source binding *MAC-ADDRESS* **vlan** *VLAN-ID IPV6-ADDRESS* **interface** *INTERFACE-ID*

Параметры

MAC-ADDRESS	Укажите MAC-адрес привязки, созданной вручную.
vlan *VLAN-ID*	Укажите VLAN привязки, созданной вручную.
IPV6-ADDRESS	Укажите IPv6-адрес привязки, созданной вручную.
interface *INTERFACE-ID*	Укажите номер интерфейса привязки, созданной вручную.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для добавления статической записи в таблицу привязок вручную.

Пример

В данном примере показано, как настроить привязку IPv6 Source Guard с IPv6-адресом 2000::1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 на интерфейсе Ethernet 1/0/10.

```
Switch#configure terminal
Switch(config)#ipv6 source binding 00-01-02-03-04-05 vlan 2 2000::1 interface eth1/0/1
Switch(config)#
```

38.2 ipv6 source-guard policy

Данная команда используется для создания политики IPv6 Source Guard. Команда позволяет войти в режим IPv6 Source-Guard Policy Configuration Mode. Для удаления политики Pv6 Source Guard воспользуйтесь формой **no** этой команды.

ipv6 source-guard policy *POLICY-NAME*
no ipv6 source-guard policy *POLICY-NAME*

Параметры

POLICY-NAME	Укажите имя политики IPv6 Source Guard.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для создания/удаления политики IPv6 Source Guard. Команда позволяет войти в режим IPv6 Source-Guard Policy Configuration Mode.

Пример

В данном примере показано, как создать политику IPv6 Source Guard.

```
Switch#configure terminal
Switch(config)#ipv6 source-guard policy policy1
Switch(config-source-guard)#
```

38.3 deny global-autoconfig

Данная команда используется для запрета трафика от автоматически сконфигурированных глобальных адресов. Для отключения функции воспользуйтесь формой **no** этой команды.

deny global-autoconfig
no deny global-autoconfig

Параметры

Нет.

По умолчанию

По умолчанию данная опция разрешена.

Режим ввода команды

Source-guard Policy Configuration Mode.

Использование команды

Данная команда используется для запрета трафика от автоматически сконфигурированных глобальных адресов. Рекомендуется к применению, если все глобальные адреса назначены DHCP и администратор хочет заблокировать входящий трафик от узлов с самостоятельно сконфигурированными адресами.

Пример

В данном примере показано, как запретить автоматически сконфигурированный трафик.

```
Switch#configure terminal
Switch(config)#ipv6 source-guard policy policy1
Switch(config-source-guard)#deny global-autoconfig
Switch(config-source-guard)#
```

38.4 permit link-local

Данная команда используется для аппаратного разрешения трафика данных, отправленных с адреса Link-Local. Для отключения данной функции воспользуйтесь формой **no** этой команды.

permit link-local
no permit link-local

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Source-guard Policy Configuration Mode.

Использование команды

Данная команда используется для аппаратного разрешения трафика данных, отправленных с адреса Link-Local.

Пример

В данном примере показано, как разрешить весь трафик данных, отправленных с адреса Link-Local.

```
Switch#configure terminal
Switch(config)#ipv6 source-guard policy policy1
Switch(config-source-guard)#permit link-local
Switch(config-source-guard)#
```

38.5 ipv6 source-guard attach-policy

Данная команда используется для применения IPv6 Source Guard на интерфейсе. Чтобы отменить применение IPv6 Source Guard на интерфейсе, воспользуйтесь формой **no** этой команды.

ipv6 source-guard attach-policy [*POLICY-NAME***]**
no ipv6 source-guard attach-policy

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики Source Guard.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.

Если команда применена к порту, будет выполнена проверка привязки адреса для полученного IPv6-пакета, кроме ND, RA, RS и DHCP-сообщений. Пакет будет разрешен, если он соответствует любой записи в таблице привязок адресов. Таблица привязок включает в себя динамическую таблицу (созданную с помощью команд IPv6 Snooping) и статическую таблицу (созданную с помощью команды **ipv6 source binding vlan**).

Если имя политики не указано, используемая по умолчанию политика Source Guard разрешит пакеты, отправленные с автоматически сконфигурированного адреса, и запретит пакеты, отправленные с адреса Link-Local.

Пример

В данном примере показано, как применить политику IPv6 Source Guard «pol1» на интерфейсе Ethernet 1/0/3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ipv6 source-guard attach-policy pol1
Switch(config-if)#
```

38.6 show ipv6 source-guard policy

Данная команда используется для просмотра настроек политики IPv6 Source Guard.

show ipv6 source-guard policy [*POLICY-NAME***]**

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики Source Guard.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для просмотра настроек политики IPv6 Source Guard. Если имя политики не указано, отображаться будет информация для всех политик IPv6 Source Guard.

Пример

В данном примере показано, как включить отображение настроек для политики IPv6 Source Guard.

```
Switch# show ipv6 source-guard policy

Policy Test configuration:
    permit link-local
    deny global-autoconf
    Target: eth1/0/3

Switch#
```

38.7 show ipv6 neighbor binding

Данная команда используется для просмотра таблицы привязок IPv6.

show ipv6 neighbor binding [vlan *VLAN-ID***] [interface** *INTERFACE-ID***] [ipv6** *IPV6-ADDRESS***] [mac** *MAC-ADDRESS***]**

Параметры

vlan *VLAN-ID*	(Опционально.) Укажите для отображения привязок, соответствующих указанной VLAN.
interface *INTERFACE-ID*	(Опционально.) Укажите для отображения привязок, соответствующих указанному номеру интерфейса.
ipv6 *IPV6-ADDRESS*	(Опционально.) Укажите для отображения привязок, соответствующих указанному IPv6-адресу.
mac *MAC-ADDRESS*	(Опционально.) Укажите для отображения привязок, соответствующих указанному MAC-адресу.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Команда используется для просмотра таблицы привязок.

Пример

В данном примере показано, как включить отображение указанных записей из таблицы привязок.

```
Switch#
show ipv6 neighbor binding

Codes: D - DHCPv6 Snooping, S - Static, N - ND Snooping
  IPv6 address                MAC address    Interface       VLAN Time left
N FE80::A8BB:CCFF:FE01:F500   AABB.CC01.F500 eth1/0/1        100  8850
S FE80::21D:71FF:FE99:4900    001D.7199.4900 eth1/0/1        100  N/A
N 2001:600::1                 AABB.CC01.F500 eth1/0/2        100  3181
D 2001:300::1                 AABB.CC01.F500 Port-channel3   100  9559
D 2001:100::2                 AABB.CC01.F600 eth1/0/1        200  9196
D 2001:400::1                 001D.7199.4900 eth1/0/2        100  1568
S 2001:500::1                 000A.000B.000C eth1/0/13       300  N/A

Total Entries: 7

Switch#
```

Отображаемые параметры

Codes	Коды для IPv6 Snooping Owner **D**: DHCPv6 Snooping **S**: Статический **N**: ND Snooping
IPv6 address	IPv6-адрес привязки.
MAC address	MAC-адрес привязки.
Interface	Номер интерфейса привязки.
VLAN	VLAN привязки.
Time left	Оставшееся время жизни привязки. Период отсутствия активности для статической привязки.

39. Команды Link Aggregation Control Protocol (LACP)

39.1 channel-group

Данная команда используется для привязки интерфейса к агрегированной группе (channel-group). Для удаления интерфейса из агрегированной группы (channel-group) используйте форму **no**.

channel-group *CHANNEL-NO* **mode {on | active | passive}**
no channel-group

Параметры

CHANNEL-NO	Укажите channel-group ID. Доступный диапазон значений: от 1 до 32.
on	Укажите интерфейс в качестве статического участника channel-group.
active	Укажите, чтобы включить для интерфейса режим LACP Active Mode.
passive	Укажите, чтобы включить для интерфейса режим LACP Passive Mode.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для конфигурирования физических портов. При первом подключении порта к channel-group система автоматически создаст port-channel. Интерфейс может подключиться только к одной channel-group.

Если в команде указан параметр **on**, тип channel-group – статическая. Если в команде указан параметр **active** или **passive**, тип channel-group – LACP. Channel-group может состоять только или из статических участников, или из участников LACP. После того как тип channel-group был определен, интерфейсы других типов не смогут подключиться к channel-group.

Используйте форму **no** данной команды, чтобы удалить интерфейс из channel-group. Если после удаления порта в channel-group не осталось портов-участников, она автоматически будет удалена. Port-channel также можно удалить при помощи команды **no interface port-channel**.

Если на порту включена функция Security, данный порт нельзя указать в качестве участника channel-group.

Пример

В данном примере показано, как привязать интерфейсы от Ethernet 1/0/4 до Ethernet 1/0/5 к новой LACP channel-group с ID 3 и включить режим LACP Active Mode.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/4-5
Switch(config-if)#channel-group 3 mode active
Switch(config-if)#
```

39.2 lacp port-priority

Данная команда используется для настройки приоритета порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

lacp port-priority *PRIORITY*
no lacp port-priority

Параметры

PRIORITY	Укажите приоритет порта в диапазоне от 1 до 65535.

По умолчанию

Приоритет порта по умолчанию – 32768.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Приоритет порта LACP определяет, какие порты могут подключиться к port-channel и на каких портах включен режим Standalone Mode. Чем ниже значение, тем выше приоритет. Если у двух и более портов совпадает приоритет, то приоритет будет определяться номером порта.

Пример

В данном примере показано, как сконфигурировать приоритет порта на интерфейсах от Ethernet 1/0/4 до Ethernet 1/0/5. Указанное значение – 20000.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/4-5
Switch(config-if)#lacp port-priority 20000
Switch(config-if)#
```

39.3 lacp timeout

Данная команда используется для настройки таймера LACP Long или LACP Short. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

lacp timeout {short | long}
no lacp timeout

Параметры

short	Укажите, чтобы выбрать значение 3 секунды для интервала, по истечении которого полученная информация о LACPDU будет объявлена недействительной. После того как партнер распознает в полученном PDU данную информацию, регулярные передачи LACP PDU будут выполняться с интервалом в 1 секунду.

long	Укажите, чтобы выбрать значение 90 секунд для интервала, по истечении которого полученная информация о LACPDU будет объявлена недействительной. После того как партнер распознает в полученном PDU данную информацию, регулярные передачи LACP PDU будут выполняться с интервалом в 30 секунд.

По умолчанию

Режим LACP Timeout по умолчанию – Short.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Используйте данную команду для конфигурирования физических портов.

Пример

В данном примере показано, как сконфигурировать режим LACP Timeout Long на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lacp timeout long
Switch(config-if)#
```

39.4 lacp system-priority

Данная команда используется для настройки приоритета системы. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

lacp system-priority *PRIORITY*
no lacp system-priority

Параметры

PRIORITY	Укажите приоритет системы в диапазоне от 1 до 65535.

По умолчанию

Приоритет системы LACP по умолчанию – 32768.

Режим ввода команды

Global Configuration Mode.

Использование команды

Во время LACP-согласования локальный партнер обменивается с удаленным партнером приоритетом системы и приоритетом порта. Если максимальное количество участников превышает ограничение, при помощи приоритета порта коммутатор определяет, в каком режиме функционирует порт –

Backup Mode или Active Mode. Приоритет системы LACP определяет коммутатор, контролирующий приоритет порта. Приоритеты портов других коммутаторов будут игнорированы.

Чем ниже значение, тем выше приоритет. Если у двух коммутаторов совпадает приоритет системы, приоритет будет определяться при помощи ID/MAC системы LACP. Команда приоритета системы LACP применима для всех LACP port-channel коммутатора.

Пример

В данном примере показано, как сконфигурировать приоритет системы LACP. Указанное значение – 30000.

```
Switch#configure terminal
Switch(config)#lacp system-priority 30000
Switch(config)#
```

39.5 port-channel load-balance

Данная команда используется для настройки алгоритма Load Balancing (балансировка нагрузки), используемого коммутатором для распределения пакетов на порты одного канала. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}
no port-channel load-balance

Параметры

dst-ip	Укажите, чтобы коммутатор проверил IP-адрес назначения (destination).
dst-mac	Укажите, чтобы коммутатор проверил MAC-адрес назначения.
src-dst-ip	Укажите, чтобы коммутатор проверил IP-адрес источника (source) и IP-адрес назначения.
src-dst-mac	Укажите, чтобы коммутатор проверил MAC-адрес источника и MAC-адрес назначения.
src-ip	Укажите, чтобы коммутатор проверил IP-адрес источника.
src-mac	Укажите, чтобы коммутатор проверил MAC-адрес источника.

По умолчанию

Алгоритм Load Balancing по умолчанию – **src-dst-mac**.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы указать алгоритм Load Balancing. Можно указать только один алгоритм.

Пример

В данном примере показано, как сконфигурировать алгоритм Load Balancing **src-ip**.

```
Switch#configure terminal
Switch(config)#port-channel load-balance src-ip
Switch(config)#
```

39.6 show channel-group

Данная команда используется для отображения информации о channel-group.

show channel-group [channel [*CHANNEL-NO*] {detail | neighbor} | load-balance | sys-id]

Параметры

channel	(Опционально.) Укажите, чтобы отобразить информацию для указанных port-channel.
CHANNEL-NO	(Опционально.) Укажите channel-group ID.
detail	(Опционально) Укажите, чтобы отобразить подробную информацию о channel-group.
neighbor	(Опционально.) Укажите, чтобы отобразить информацию о соседнем устройстве.
load-balance	(Опционально.) Укажите, чтобы отобразить информацию о балансировке нагрузки.
sys-id	(Опционально.) Укажите, чтобы отобразить system identifier, используемый LACP.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если номер port-channel не указан, будут отображены все port-channel. Если в команде **show channel-group** не указаны параметры, будет отображена только краткая информация о channel-group.

Пример

В данном примере показано, как отобразить подробную информацию обо всех port-channel.

```
Switch# show channel-group channel detail

Flag:
  S - Port is requesting Slow LACPDUs   F - Port is requesting fast LACPDU
  A - Port is in active mode            P - Port is in passive mode
LACP state:
  bndl:     Port is attached to an aggregator and bundled with other ports.
  hot-sby:  Port is in a hot-standby state.
  indep:    Port is in an independent state(not bundled but able to switch data
            traffic)
  down:     Port is down.

Channel Group 1
  Member Ports: 2, Maxports = 8, Protocol: LACP
  Description:
                       LACP         Port       Port
  Port          Flags  State        Priority   Number
  ------------------------------------------------
  eth1/0/10     SA     bndl         32768      10
  eth1/0/11     SA     bndl         32768      11

Channel Group 2
  Member Ports: 2, Maxports = 8, Protocol: Static
                       LACP         Port       Port
  Port          Flags  State        Priority   Number
  ------------------------------------------------
  eth1/0/8      N/A    bndl         N/A        N/A
  eth1/0/9      N/A    down         N/A        N/A

Switch#
```

В данном примере показано, как отобразить информацию о соседнем устройстве для port-channel 3.

```
Switch# show channel-group channel 3 neighbor

Flag:
  S - Port is requesting Slow LACPDUs   F - Port is requesting fast LACPDU
  A - Port is in active mode            P - Port is in passive mode

Channel Group 3
               Partner                  Partner   Partner   Partner
  Port         System ID                PortNo    Flags     Port_Pri
  ---------------------------------------------------------------------
  eth1/0/1     32768,F8-E9-80-1F-23-90  12        SP        32768
  eth1/0/2     32768,F8-E9-80-1F-23-90  13        SP        32768

Switch#
```

В данном примере показано, как отобразить информацию о балансировке нагрузки для всех channel-group.

```
Switch#show channel-group load-balance

load-balance algorithm: src-dst-mac

Switch#
```

В данном примере показано, как отобразить информацию о system identifier.

```
Switch# show channel-group sys-id

System-ID: 32765,00-02-4B-29-3A-00

Switch#
```

В данном примере показано, как отобразить краткую информацию обо всех port-channel.

```
Switch# show channel-group

load-balance algorithm: src-dst-mac
System-ID: 32768,3C-1E-04-A1-CC-00

Group          Protocol
-----------------------
1              LACP
2              Static

Switch#
```

40. Команды Link Layer Discovery Protocol (LLDP)

40.1 clear lldp counters

Данная команда используется для удаления статистики LLDP.

clear lldp counters [all | interface *INTERFACE-ID* **[, | -]]**

Параметры

all	(Опционально.) Укажите, чтобы обнулить счетчик LLDP для всех интерфейсов и статистики Global LLDP.
interface *INTERFACE-ID*	(Опционально.) Укажите интерфейс, на котором необходимо обнулить счетчик LLDP.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, указав параметр **interface**, чтобы сбросить счетчик статистики LLDP на выбранном интерфейсе/интерфейсах. Используйте команду **clear lldp counters**, указав параметр **all**, чтобы удалить статистику LLDP и Global LLDP на всех интерфейсах. Если не указаны дополнительные параметры, будут обнулены только счетчики Global LLDP.

Пример

В данном примере показано, как удалить всю статистику LLDP.

```
Switch#clear lldp counters all
Switch#
```

40.2 clear lldp table

Данная команда используется для удаления всей информации об LLDP, полученной от соседних устройств.

clear lldp table {all | interface *INTERFACE-ID* **[, | -]}**

Параметры

all	Укажите, чтобы удалить информацию об LLDP, полученную от соседних устройств, для всех интерфейсов.
interface *INTERFACE-ID*	Укажите интерфейсы, которые необходимо удалить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если в команде указан параметр **interface**, будет удалена информация, полученная от соседних устройств, на указанных интерфейсах. Используйте команду, указав параметр **all**, чтобы удалить всю информацию, полученную от соседних устройств.

Пример

В данном примере показано, как удалить всю информацию, полученную от соседних устройств, на всех интерфейсах.

```
Switch#clear lldp table all
Switch#
```

40.3 lldp dot1-tlv-select

Данная команда используется для указания дополнительных настроек TLV (type-length-value) в указанном в пределах IEEE 802.1 наборе TLV, которые будут переданы и инкапсулированы в LLDPDU, а затем отправлены на соседние устройства. Для отключения передачи TLV используйте форму **no**.

lldp dot1-tlv-select {port-vlan | vlan-name [*VLAN-ID* **[, | -]] | protocol-identity [***PROTOCOL-NAME***]}**

no lldp dot1-tlv-select {port-vlan | vlan-name [*VLAN-ID* **[, | -]] | protocol-identity [***PROTOCOL-NAME***]}**

Параметры

port-vlan	Укажите Port VLAN ID TLV, который необходимо отправить. Port VLAN ID TLV – это дополнительный TLV фиксированной длины, который позволяет порту VLAN Bridge анонсировать PVID (Port VLAN Identifier), который будет ассоциирован с нетегированными или тегированными по приоритету кадрами.

vlan-name	Укажите VLAN Name TLV, который необходимо отправить. VLAN Name TLV – это дополнительный TLV, который позволяет IEEE 802 LAN station, совместимой с IEEE 802.1Q, анонсировать присвоенное имя любой VLAN, с которой она сконфигурирована.
VLAN-ID	(Опционально.) Укажите VLAN ID в VLAN Name TLV. Доступный диапазон значений: от 1 до 4094. Если VLAN ID не указан, все сконфигурированные VLAN для VLAN Name TLV будут удалены, VLAN Name TLV отправлен не будет.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
protocol-identity	Укажите Protocol Identity TLV, который необходимо отправить. Protocol Identity TLV – это дополнительный TLV, который позволяет IEEE 802 LAN station анонсировать определенные протоколы, доступные через порт.
PROTOCOL-NAME	(Опционально.) Укажите имя протокола. Ниже перечислены допустимые для *PROTOCOL-NAME* строки: **eapol** - Extensible Authentication Protocol (EAP) over LAN **lacp** - Link Aggregation Control Protocol **stp** - Spanning Tree Protocol

По умолчанию

По умолчанию указанные в пределах IEEE 802.1 TLV не заданы.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта. Если включено анонсирование дополнительных TLV, они будут инкапсулированы в LLDPDU и отправлены на другие устройства.

Тип Protocol Identity TLV определяет, анонсировать ли соответствующий экземпляр Protocol Identity локальной системы на порту. Protocol Identity TLV позволяет устройствам анонсировать протоколы, которые важны для работы сети. Например, такие протоколы как Spanning Tree Protocol, Link Aggregation Control Protocol и другие протоколы, установленные vendor-ом, отвечают за поддержку топологии и подключения к сети. Если работают обе функции протокола и на порту включено анонсирование Protocol Identity, Protocol Identity TLV будет анонсирован.

VLAN будет анонсирована в VLAN Name TLV только при условии, что интерфейс является портом-членом сконфигурированного VLAN ID.

Пример

В данном примере показано, как включить анонсирование Port VLAN ID TLV.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp dot1-tlv-select port-vlan
Switch(config-if)#
```

В данном примере показано, как включить анонсирование VLAN Name TLV. Анонсированные VLAN: от VLAN 1 до VLAN 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp dot1-tlv-select vlan-name 1-3
Switch(config-if)#
```

В данном примере показано, как включить анонсирование LACP Protocol Identity TLV.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp dot1-tlv-select protocol-identify lacp
Switch(config-if)#
```

40.4 lldp dot3-tlv-select

Данная команда используется для указания дополнительных настроек TLV в указанном в пределах IEEE 802.3 наборе TLV, которые будут инкапсулированы в LLDPDU, а затем отправлены на соседние устройства. Для отключения передачи TLV воспользуйтесь формой **no** этой команды.

lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | max-frame-size]

no lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | max-frame-size]

Параметры

mac-phy-cfg	(Опционально.) Укажите MAC/PHY Configuration/Status TLV, который необходимо отправить. MAC/PHY Configuration/Status TLV – это дополнительный TLV, который определяет (1) режим дуплекса и максимальную скорость передачи узла EEE 802.3 LAN в бит/сек, а также (2) текущий режим дуплекса и настройки скорости передачи узла IEEE 802.3 LAN в бит/сек.
link-aggregation	(Опционально.) Укажите Link Aggregation TLV, который необходимо отправить. Link Aggregation TLV содержит информацию о том, можно ли агрегировать группу, агрегируется ли группа в данный момент, а также информацию об агрегированном port channel ID. Если порт не агрегирован, значение port channel ID – 0.
max-frame-size	(Опционально.) Укажите Maximum Frame Size TLV, который необходимо отправить. Maximum Frame Size TLV указывает максимальный размер кадра для используемого MAC и PHY.

По умолчанию

По умолчанию указанный в пределах IEEE 802.3 TLV не выбран.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.

Если при помощи данной команды включено анонсирование дополнительных TLV, указанных в пределах IEEE 802.3, они будут инкапсулированы в LLDPDU и отправлены на другие устройства.

Пример

В данном примере показано, как включить анонсирование MAC/PHY Configuration/Status TLV.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp dot3-tlv-select mac-phy-cfg
Switch(config-if)#
```

40.5 lldp fast-count

Данная команда используется для настройки количества отправляемых пакетов Fast Start (LLDP MED Fast Start Repeat Count Option) на коммутаторе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

lldp fast-count *VALUE*

no lldp fast-count

Параметры

VALUE	Укажите количество отправляемых пакетов Fast Start. Доступный диапазон значений: от 1 до 10.

По умолчанию

Значение по умолчанию – 4.

Режим ввода команды

Global Configuration Mode.

Использование команды

При обнаружении LLDP MED Capabilities TLV будет запущена процедура Fast Start. Используйте данную команду, чтобы настроить количество отправляемых пакетов Fast Start, которое соответствует количеству передач LLDP-сообщений за один полный интервал Fast Start.

Пример

В данном примере показано, как сконфигурировать количество отправляемых пакетов Fast Start.

```
Switch#configure terminal
Switch(config)#lldp fast-count 10
Switch(config)#
```

40.6 lldp hold-multiplier

Данная команда используется для того, чтобы настроить множитель удержания для обновлений LLDP на коммутаторе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

lldp hold-multiplier *VALUE*
no hold-multiplier

Параметры

VALUE	Укажите множитель для интервала передачи LLDPDU, с помощью которого будет вычислено значение TTL для LLDPDU. Доступный диапазон значений: от 2 до 10.

По умолчанию

Значение по умолчанию – 4.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данный параметр – это множитель для интервала передачи LLDPDU, с помощью которого будет вычислено значение TTL в LLDPDU. Время жизни определяется при помощи множителя удержания, умноженного на интервал TX. Если TTL для определенного анонса на соседнем коммутаторе истек, анонсированная информация будет удалена из MIB соседнего устройства.

Пример

В данном примере показано, как указать значение 3 для множителя удержания LLDP.

```
Switch#configure terminal
Switch(config)#lldp hold-multiplier 3
Switch(config)#
```

40.7 lldp management-address

Данная команда используется для настройки адреса управления (Management Address), который будет анонсирован на физическом интерфейсе. Для удаления заданных настроек воспользуйтесь формой **no** этой команды.

lldp management-address [*IP-ADDRESS* **|** *IPV6-ADDRESS***]**
no lldp management-address [*IP-ADDRESS* **|** *IPV6-ADDRESS***]**

Параметры

IP-ADDRESS	(Опционально.) Укажите IPv4-адрес, передаваемый в Management Address TLV.
IPV6-ADDRESS	(Опционально.) Укажите IPv6-адрес, передаваемый в Management Address TLV.

По умолчанию

По умолчанию адрес управления LLDP не настроен (Management Address TLV не отправляется).

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта. Используйте данную команду, чтобы указать IPv4/IPv6-адрес, передаваемый в Management Address TLV на указанном порту. Если IP-адрес указан, но адрес не ассоциирован с одним из интерфейсов системы, адрес не будет отправлен.

Если при использовании команды **lldp management-address** не указан ни один адрес, коммутатор обнаружит по крайней мере один IPv4/IPv6-адрес в VLAN с самым низким VLAN ID. Если подходящих IPv4/IPv6-адресов нет, Management Address TLV анонсирован не будет. После того как администратор сконфигурировал адрес, оба адреса управления по умолчанию (IPv4 и IPv6) станут неактивны и не будут отправлены. IPv4/IPv6-адрес по умолчанию снова станет активен, если все сконфигурированные адреса будут удалены. Используйте данную команду несколько раз, чтобы создать несколько адресов управления IPv4/IPv6.

Используйте команду **no lldp management-address** без адреса управления, чтобы отключить адрес управления, анонсированный в LLDPDU. При отсутствии в списке действительного адреса управления, Management Address TLV отправлен не будет.

Пример

В данном примере показано, как настроить адрес управления IPv4 на интерфейсах Ethernet 1/0/1-1/0/3.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/1-3
Switch(config-if-range)#lldp management-address 10.1.1.1
Switch(config-if-range)#
```

В данном примере показано, как настроить адрес управления IPv6 на интерфейсах Ethernet 1/0/4-1/0/6.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/4-6
Switch(config-if-range)#lldp management-address FE80::250:A2FF:FEBF:A056
Switch(config-if-range)#
```

В данном примере показано, как удалить адрес управления IPv4 из интерфейсов Ethernet 1/0/1-Ethernet 1/0/3.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/1-3
Switch(config-if-range)#no lldp management-address 10.1.1.1
Switch(config-if-range)#
```

В данном примере показано, как удалить адрес управления IPv6 из интерфейсов Ethernet 1/0/4-Ethernet 1/0/6.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/4-6
Switch(config-if-range)#no lldp management-address FE80::250:A2FF:FEBF:A056
Switch(config-if-range)#
```

В данном примере показано, как удалить все адреса управления IPv4/IPv6 из интерфейса Ethernet 1/0/5. В этом случае с Ethernet 1/0/5 Management Address TLV отправлен не будет.

```
Switch#configure terminal
Switch(config)#interface eth1/0/5
Switch(config-if)#no lldp management-address
Switch(config-if)#
```

40.8 lldp med-tlv-select

Данная команда используется для указания дополнительного LLDP-MED TLV, который будет передан, инкапсулипрован в LLDPDU и отправлен на соседние устройства. Для отключения передачи TLV воспользуйтесь формой **no** этой команды.

lldp med-tlv-select [capabilities | inventory-management | network-policy]
no lldp med-tlv-select [capabilities | inventory-management | network-policy]

Параметры

capabilities	(Опционально.) Укажите, чтобы передать LLDP-MED Capabilities TLV.
inventory-management	(Опционально.) Укажите, чтобы передать LLDP-MED Inventory Management TLV.
network-policy	(Опционально.) Укажите, чтобы передать LLDP-MED Network Policy TLV.

По умолчанию

LLDP-MED TLV по умолчанию не выбран.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.

Команда применяется для включения/отключения передачи LLDP-MED TLV. При отключении передачи Capabilities TLV будут также отключены LLDP-MED на физическом интерфейсе: LLDP-MED TLV не будут отправляться, даже если другие LLDP-MED TLV включены.

По умолчанию коммутатор отправляет LLDP-пакеты до тех пор, пока получает пакеты LLDP-MED от конечного устройства. Коммутатор отправляет пакеты LLDP-MED до тех пор, пока получает LLDP-пакеты.

Пример

В данном примере показано, как включить передачу LLDP-MED TLV и LLDP-MED Capabilities TLV.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp med-tlv-select capabilities
Switch(config-if)#
```

40.9 lldp receive

Данная команда используется для того, чтобы включить на физическом интерфейсе получение LLDP-сообщений. Используйте форму **no**, чтобы отключить получение LLDP-сообщений.

lldp receive
no lldp receive

Параметры

Нет.

По умолчанию

По умолчанию функция LLDP включена на всех поддерживаемых интерфейсах.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки физических портов.

Команда применяется для того, чтобы включить на интерфейсе получение LLDP-сообщений. Если LLDP не включен, коммутатор не будет получать LLDP-сообщения.

Пример

В данном примере показано, как включить на физическом интерфейсе получение LLDP-сообщений.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp receive
Switch(config-if)#
```

40.10 lldp reinit

Данная команда используется для настройки минимального интервала перед повторной инициализацией на коммутаторе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

lldp reinit *SECONDS*
no lldp reinit

Параметры

SECONDS	Укажите время задержки инициализации LLDP на интерфейсе. Доступный диапазон значений: от 1 до 10 секунд.

По умолчанию

Значение по умолчанию – 2 секунды.

Режим ввода команды

Global Configuration Mode.

Использование команды

При перезапуске физического интерфейса LLDP будет выдержан заданный интервал времени между последней командой disable и повторной инициализацией.

Пример

В данном примере показано, как сконфигурировать интервал перед повторной инициализацией. Указанное значение – 5 секунд.

```
Switch#configure terminal
Switch(config)#lldp reinit 5
Switch(config)#
```

40.11 lldp run

Данная команда используется для глобального включения функции LLDP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

lldp run
no lldp run

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы глобально включить функцию LLDP и инициировать передачу, получение и обработку LLDP-пакетов на коммутаторе. Используйте команду **lldp transmit**, чтобы

контролировать передачу LLDP-пакетов, и команду **lldp receive**, чтобы контролировать получение LLDP-пакетов. Обе команды применяются в режиме Interface Configuration Mode. Для корректной работы на физическом интерфейсе необходимо включить LLDP как на физическом интерфейсе, так и глобально.

При анонсировании LLDP-пакетов коммутатор передает информацию соседним устройствам через физические интерфейсы. Коммутатор изучает информацию об управлении и возможности подключения, содержащуюся в LLDP-пакетах, анонсированных соседними устройствами.

Пример

В данном примере показано, как включить функцию LLDP.

```
Switch#configure terminal
Switch(config)#lldp run
Switch(config)#
```

40.12 lldp forward

Данная команда используется для включения состояния LLDP Forwarding. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

lldp forward
no lldp forward

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная функция глобально контролирует передачу LLDP. Если состояние LLDP Global отключено, а функция LLDP Forwarding включена, полученный LLDPDU-пакет будет передан.

Пример

В данном примере показано, как включить состояние LLDP Forwarding глобально.

```
Switch#configure terminal
Switch(config)#lldp forward
Switch(config)#
```

40.13 lldp tlv-select

Данная команда используется для выбора TLV в наборе 802.1AB Basic Management, а также для передачи TLV и его инкапсулирования в LLDPDU с последующей отправкой на соседние устройства. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

lldp tlv-select [port-description | system-capabilities | system-description | system-name]
no lldp tlv-select [port-description | system-capabilities | system-description | system-name]

Параметры

port-description	(Опционально.) Укажите Port Description TLV, который необходимо отправить. Port Description TLV позволяет анонсировать описание порта IEEE 802 LAN station.
system-capabilities	(Опционально.) Укажите System Capabilities TLV, который необходимо отправить. Поле System Capabilities будет содержать bit-map, определяющий основные функции системы.
system-description	(Опционально.) Укажите System Description TLV, который необходимо отправить. System Description должно включать полное имя и версию аппаратного обеспечения, операционной системы и программного обеспечения.
system-name	(Опционально.) Укажите System Name TLV, который необходимо отправить. System Name должно представлять собой полное имя домена системы.

По умолчанию

По умолчанию дополнительный 802.1AB Basic Management TLV не указан.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки физических портов.

Команда применяется для выбора дополнительных TLV, которые необходимо передать. Если выбрано анонсирование дополнительных TLV, они будут инкапсулированы в LLDPDU и отправлены на другие устройства.

Пример

В данном примере показано, как включить все поддерживаемые дополнительные 802.1AB Basic Management TLV.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp tlv-select
Switch(config-if)#
```

В данном примере показано, как включить анонсирование System Name TLV.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp tlv-select system-name
Switch(config-if)#
```

40.14 lldp transmit

Данная команда используется для включения анонсирования/передачи LLDP. Для отключения передачи LLDP воспользуйтесь формой **no** этой команды.

lldp transmit
no lldp transmit

Параметры

Нет.

По умолчанию

По умолчанию передача LLDP включена на всех поддерживаемых интерфейсах.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.

Команда применяется для включения передачи LLDP на физическом интерфейсе. Если LLDP не функционирует, коммутатор не будет передавать LLDP-сообщения.

Пример

В данном примере показано, как включить передачу LLDP.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp transmit
Switch(config-if)#
```

40.15 lldp tx-delay

Данная команда используется для настройки таймера Transmission Delay, определяющего минимальный интервал между отправкой LLDP-сообщений на основе постоянно изменяющегося содержания MIB. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

lldp tx-delay *SECONDS*
no lldp tx-delay

Параметры

SECONDS	Укажите время задержки для отправки последовательных LLDPDU

	на интерфейсе. Доступный диапазон значений: от 1 до 8192 секунд, при этом указанное значение не должно превышать одну четвертую значения таймера Transmission Interval.

По умолчанию

Значение по умолчанию – 2 секунды.

Режим ввода команды

Global Configuration Mode.

Использование команды

Значение LLDP Transmission Interval должно быть больше или равно значению таймера Transmission Delay, умноженному на четыре.

Пример

В данном примере показано, как указать значение таймера Transmission Delay. Заданное значение – 8 секунд.

```
Switch#configure terminal
Switch(config)#lldp tx-delay 8
Switch(config)#
```

40.16 lldp tx-interval

Данная команда используется для настройки интервала LLDPDU Transmission. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

lldp tx-interval *SECONDS*
no lldp tx-interval

Параметры

SECONDS	Укажите интервал между отправкой последовательных анонсов LLDPD на каждом физическом интерфейсе. Доступный диапазон значений: от 5 до 32768 секунд.

По умолчанию

Значение по умолчанию – 30 секунд.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данный интервал определяет скорость передачи LLDP-пакетов.

Пример

В данном примере показано, как сконфигурировать отправку обновлений LLDP через каждые 50 секунд.

```
Switch#configure terminal
Switch(config)#lldp tx-interval 50
Switch(config)#
```

40.17 snmp-server enable traps lldp

Данная команда используется для включения отправки LLDP Trap и LLDP-MED Trap. Для отключения данной функции воспользуйтесь формой **no** этой команды.

snmp-server enable traps lldp [med]
no snmp-server enable traps lldp [med]

Параметры

med	(Опционально.) Укажите, чтобы включить отправку LLDP-MED Trap.

По умолчанию

По умолчанию отправка LLDP Trap и LLDP-MED Trap отключены.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте команду **snmp-server enable traps lldp**, чтобы включить отправку LLDP-уведомлений.

Используйте команду **ssnmp-server enable traps lldp med**, чтобы включить отправку LLDP-MED-уведомлений.

Пример

В данном примере показано, как включить отправку LLDP-MED Trap.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps lldp med
Switch(config)#
```

40.18 lldp notification enable

Данная команда используется для включения отправки уведомлений LLDP и LLDP-MED на интерфейсе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

lldp [med] notification enable
no lldp [med] notification enable

Параметры

med	(Опционально.) Укажите, чтобы включить уведомления LLDP-MED.

По умолчанию

По умолчанию уведомления LLDP и LLDP-MED отключены.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Используйте команду **lldp notification enable**, чтобы включить отправку уведомлений LLDP.

Используйте команду **lldp med notification enable**, чтобы включить отправку уведомлений LLDP-MED.

Пример

В данном примере показано, как включить отправку уведомлений LLDP-MED для интерфейса Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp med notification enable
Switch(config-if)#
```

40.19 lldp subtype

Данная команда используется для настройки подтипа LLDP TLV.

lldp subtype port-id {mac-address | local}

Параметры

port-id	Укажите подтип Port ID TLV.
mac-address	Укажите, чтобы обозначить подтип Port ID TLV как «MAC Address (3)», а также чтобы закодировать MAC-адрес в поле «port ID».
local	Укажите, чтобы обозначить подтип Port ID TLV как «Locally assigned (7)», а также чтобы закодировать номер порта в поле «port ID».

По умолчанию

Подтип Port ID TLV по умолчанию – local (port number).

Режим ввода команды

Interface Configuration Mode.

Использование команды

Используйте данную команду, чтобы указать подтип LLDP TLV. Подтип Port ID указывает, как обозначен порт в поле port ID.

Пример

В данном примере показано, как сконфигурировать подтип Port ID TLV. Указанный подтип – mac-address.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp subtype port-id mac-address
Switch(config-if)#
```

40.20 show lldp

Данная команда используется для отображения общих настроек функции LLDP на коммутаторе.

show lldp

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить общие настройки функции LLDP на коммутаторе.

Пример

В данном примере показано, как отобразить общие настройки функции LLDP на коммутаторе.

```
Switch#show lldp

LLDP System Information
    Chassis ID Subtype        : MAC Address
    Chassis ID                : F0-7D-68-12-10-01
    System Name               : Switch
    System Description        : 10 Gigabit Ethernet Smart Managed Switch
    System Capabilities Supported: Repeater, Bridge
    System Capabilities Enabled  : Repeater, Bridge
LLDP-MED System Information:
    Device Class              : Network Connectivity Device
    Hardware Revision         : A1
    Firmware Revision         :
    Software Revision         : 1.00.021
    Serial Number             : DXS1210102030
    Manufacturer Name         : D-Link Corporation
    Model Name                : DXS-1210-28T
    Asset ID                  :

LLDP Configurations
    LLDP State                : Disabled
    LLDP Forward State        : Disabled
    Message TX Interval       : 30
    Message TX Hold Multiplier: 4
    ReInit Delay              : 2
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

40.21 show lldp interface

Данная команда используется для того, чтобы отобразить настройки функции LLDP на физическом интерфейсе.

show lldp interface *INTERFACE-ID* **[, | -]**

Параметры

INTERFACE-ID	Укажите интерфейс, который необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.

Используйте данную команду, чтобы отобразить информацию о функции LLDP для каждого физического интерфейса.

Пример

В данном примере показано, как отобразить настройки функции LLDP для интерфейса Ethernet 1/0/1.

```
Switch# show lldp interface eth1/0/1

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID                                                 :eth1/0/1
Admin Status                                            :TX and RX
Notification                                            :Disabled
Basic Management TLVs:
    Port Description                                    :Disabled
    System Name                                         :Disabled
    System Description                                  :Disabled
    System Capabilities                                 :Disabled
    Enabled Management Address:
        (None)
IEEE 802.1 Organizationally Specific TLVs:

    Port VLAN ID                                        :Disabled
    Enabled Port_and_Protocol_VLAN_ID
        (None)
    Enabled VLAN Name
        (None)
    Enabled Protocol_Identity
        (None)
IEEE 802.3 Organizationally Specific TLVs:

    MAC/PHY Configuration/Status                        :Disabled
    Power Via MDI                                       :Disabled
    Link Aggregation                                    :Disabled
    Maximum Frame Size                                  :Disabled

LLDP-MED Organizationally Specific TLVs:

    LLDP-MED Capabilities TLV                           :Disabled
    LLDP-MED Network Policy TLV                         :Disabled
    LLDP-MED Extended Power Via MDI PSE TLV             :Disabled
    LLDP-MED Inventory TLV                              :Disabled

Switch#
```

Отображаемые параметры

Enabled Management Address	Отображает включенные IPv4/IPv6-адреса. «(None)» означает, что пользователь не сконфигурировал адрес управления (Management Address) при помощи команды **lldp management-address** или включенные IPv4/IPv6-адреса по умолчанию не применяются.
Enabled Port and Protocol VLAN ID	Отображает включенные Port and Protocol VLAN. В список VLAN включены сконфигурированные и включенные VLAN. При отсутствии сконфигурированных PPVID VLAN отображается «(None)».
Enabled VLAN Name	Отображает включенные VLAN для отправки VLAN Name TLV. В список VLAN включены сконфигурированные и включенные VLAN. При отсутствии сконфигурированных VLAN для VLAN Name TLV отображается «(None)».
Enabled Protocol Identity	Отображает включенную строку протокола для Protocol Identity TLV. При отсутствии включенных протоколов для Protocol Identity TLV отображается «(None)».

40.22 show lldp local interface

Данная команда используется для отображения информации о физическом интерфейсе, которая будет отправлена на соседние устройства в LLDP TLV.

show lldp local interface *INTERFACE-ID* **[, | -] [brief | detail]**

Параметры

INTERFACE-ID	Укажите интерфейс, который необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
brief	(Опционально.) Укажите, чтобы отобразить информацию в сокращенном формате.
detail	(Опционально.) Укажите, чтобы отобразить информацию в подробном формате. Если не указан ни параметр **brief**, ни параметр **detail**, информация будет отображена в стандартном формате.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.

Используйте данную команду, чтобы отобразить текущую анонсируемую локальную информацию в исходящих LLDP-объявлениях для каждого физического интерфейса.

Пример

В данном примере показано, как отобразить локальную информацию для интерфейса физического порта Ethernet 1/0/1 в подробном формате.

```
Switch#show lldp local interface eth1/0/1 detail

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : eth1/0/1
Port Description                         : D-Link Corporation DXS-1210-28T HW
                                           A1 firmware 1.00.021 Port 1 on Unit
                                           1
Port PVID                                : 1
Management Address Count                 : 2

    Address 1 : (default)
        Subtype                          : IPv4
        Address                          : 10.90.90.90
        IF Type                          : IfIndex
        OID                              : 1.3.6.1.4.1.171.10.139.6.1

    Address 2 :
        Subtype                          : IPv4
        Address                          : 10.90.90.90
        IF Type                          : IfIndex
        OID                              : 1.3.6.1.4.1.171.10.139.6.1

PPVID Entries Count                      : 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

В данном примере показано, как отобразить локальную информацию для интерфейса физического порта Ethernet 1/0/1 в стандартном формате.

```
Switch#show lldp local interface eth1/0/1

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : eth1/0/1
Port Description                         : D-Link Corporation DXS-1210-28T HW
                                           A1 firmware 1.00.021 Port 1 on Unit
                                           1
Port PVID                                : 1
Management Address Count                 : 2
PPVID Entries Count                      : 0
VLAN Name Entries Count                  : 1
Protocol Identity Entries Count          : 0
MAC/PHY Configuration/Status             : (See Detail)
Link Aggregation                         : (See Detail)
Maximum Frame Size                       : 1536
LLDP-MED capabilities                    : (See Detail)
Network Policy                           : (See Detail)


Switch#
```

В данном примере показано, как отобразить локальную информацию для интерфейса физического порта Ethernet 1/0/1 в сокращенном формате.

```
Switch#show lldp local interface eth1/0/1 brief

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : eth1/0/1
Port Description                         : D-Link Corporation DXS-1210-28T HW
                                           A1 firmware 1.00.021 Port 1 on Unit
                                           1


Switch#
```

40.23 show lldp management-address

Данная команда используется для отображения информации об адресе управления (Management Address).

show lldp management-address [*IP-ADDRESS* **|** *IPV6-ADDRESS***]**

Параметры

IP-ADDRESS	(Опционально.) Укажите, чтобы отобразить информацию об LLDP Management для указанного IPv4-адреса.

IPV6-ADDRESS	(Опционально.) Укажите, чтобы отобразить информацию об LLDP Management для указанного IPv6-адреса.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить информацию об адресе управления.

Пример

В данном примере показано, как отобразить всю информацию об адресе управления.

```
Switch#show lldp management-address

Address 1 : (default)
-----------------------------------------------
    Subtype                          : IPv4
    Address                          : 10.90.90.90
    IF Type                          : IfIndex
    OID                              : 1.3.6.1.4.1.171.10.165.2.1
    Advertising Ports                : -

Address 2 :
-----------------------------------------------
    Subtype                          : IPv4
    Address                          : 10.90.90.90
    IF Type                          : IfIndex
    OID                              : 1.3.6.1.4.1.171.10.165.2.1
    Advertising Ports                : -

Total Entries : 2


Switch#
```

40.24 show lldp neighbors interface

Данная команда используется для отображения актуальной информации, полученной от соседнего устройства на указанном физическом интерфейсе.

show lldp neighbors interface *INTERFACE-ID* **[, | -] [brief | detail]**

Параметры

INTERFACE-ID	Укажите интерфейс, который необходимо отобразить.

,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
brief	(Опционально.) Укажите, чтобы отобразить информацию в сокращенном формате.
detail	(Опционально.) Укажите, чтобы отобразить информацию в подробном формате. Если не указан ни параметр **brief**, ни параметр **detail**, информация будет отображена в стандартном формате.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить информацию, полученную от соседних устройств.

Пример

В данном примере показано, как отобразить информацию о соседних устройствах, изученную LLDP на интерфейсе Ethernet 1/0/9, в подробном формате.

```
Switch# show lldp neighbors interface eth1/0/9 detail

Port ID: eth1/0/9
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                      : MAC Address
    Chassis ID                              : F0-7D-68-30-36-00
    Port ID Subtype                         : Local
    Port ID                                 : eth1/0/10
    Port Description                        :
    System Name                             :
    System Description                      :
    System Capabilities                     :
    Management Address Count                : 0
        (None)

    Port PVID                               : 0
    PPVID Entries Count                     : 0
        (None)

    VLAN Name Entries Count                 : 0
        (None)

    Protocol ID Entries Count               : 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

В примере ниже показано, как отобразить информацию о соседних устройствах, изученную LLDP на интерфейсе Ethernet 1/0/9, в стандартном формате.

```
Switch# show lldp neighbors interface eth1/0/9

Port ID: eth1/0/9
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                      : MAC Address
    Chassis ID                              : F0-7D-68-30-36-00
    Port ID Subtype                         : Local
    Port ID                                 : eth1/0/10
    Port Description                        :
    System Name                             :
    System Description                      :
    System Capabilities                     :
    Management Address Count                : 0
    Port PVID                               : 0
    PPVID Entries Count                     : 0
    VLAN Name Entries Count                 : 0
    Protocol ID Entries Count               : 0
    MAC/PHY Configuration/Status            : (None)
    Power Via MDI                           : (None)
    Link Aggregation                        : (None)
    Maximum Frame Size                      : 0
    LLDP-MED capabilities                   : (See Detail)
    Extended power via MDI                  : (See Detail)
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

В данном примере показано, как отобразить информацию о соседних устройствах на интерфейсе Ethernet 1/0/9.

```
Switch# show lldp neighbors interface eth1/0/9 brief

Port ID: eth1/0/9
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                      : MAC Address
    Chassis ID                              : F0-7D-68-30-36-00
    Port ID Subtype                         : Local
    Port ID                                 : eth1/0/10
    Port Description                        :


Switch#
```

40.25 show lldp traffic

Данная команда используется для отображения глобальной информации о трафике LLDP.

show lldp traffic

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить информацию об обнаружении соседних устройств на коммутаторе.

Пример

В данном примере показано, как отобразить глобальную информацию о трафике LLDP.

```
Switch# show lldp traffic

Last Change Time  : 0D2H6M40S
Total Inserts     : 1
Total Deletes     : 0
Total Drops       : 0
Total Ageouts     : 0

Switch#
```

Отображаемые параметры

Last Change Time	Время после последнего обновления до удаленной таблицы в днях, часах, минутах и секундах.
Total Inserts	Общее количество вставок в удаленную таблицу.
Total Deletes	Общее количество удалений из удаленной таблицы.
Total Drops	Общее количество случаев получения данных, которые не были добавлены в таблицу из-за непригодности.
Total Ageouts	Общее количество случаев удаления записей после истечения интервала Time to Live.

40.26 show lldp traffic interface

Данная команда используется для отображения информации о трафике LLDP на указанном физическом интерфейсе.

show lldp traffic interface *INTERFACE-ID* **[, | -]**

Параметры

INTERFACE-ID	Укажите интерфейсы, которые необходимо отобразить.

,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить трафик LLDP на каждом физическом интерфейсе.

Пример

В данном примере показано, как отобразить статистику для порта 1.

```
Switch# show lldp traffic interface eth1/0/1

Port ID : eth1/0/1
-------------------------------------------
    Total Transmits     : 0
    Total Discards      : 0
    Total Errors        : 0
    Total Receives      : 0
    Total TLV Discards  : 0
    Total TLV Unknowns  : 0
    Total Ageouts       : 0

Switch#
```

Отображаемые параметры

Total Transmits	Общее количество LLDP-пакетов, переданных на порту.
Total Discards	Общее количество LLDP-кадров, отброшенных на порту.
Total Errors	Количество недействительных LLDP-кадров, полученных на порту.
Total Receives	Общее количество LLDP-пакетов, полученных на порту.
Total TLV Discards	Количество отброшенных TLV.
Total TLV Unknowns	Общее количество полученных на порту LLDP TLV, тип которых находится в зарезервированном диапазоне и не распознается.
Total Ageouts	Общее количество случаев удаления записей на порту после истечения интервала Time to Live.

41. Команды Loopback Detection (LBD)

41.1 loopback-detection (Global)

Данная команда используется, чтобы включить функцию LBD (Loopback Detection) глобально. Для глобального отключения данной функции воспользуйтесь формой **no** этой команды.

loopback-detection [mode {port-based | vlan-based}]
no loopback-detection [mode]

Параметры

mode	(Опционально.) Укажите режим обнаружения.
port-based	(Опционально.) Укажите режим обнаружения петли port-based (на порту).
vlan-based	(Опционально.) Укажите режим обнаружения петли VLAN-based (в VLAN).

По умолчанию

По умолчанию данная опция отключена.
Режим обнаружения по умолчанию – port-based.

Режим ввода команды

Global Configuration Mode.

Использование команды

Обычно режим port-based используется на портах, к которым подключены пользователи, а режим VLAN-based используется на trunk-портах и гибридных портах, если соседнее устройство не поддерживает функцию LBD.

Если включен режим port-based, порт, на котором включена функция LBD, будет отправлять нетегированные пакеты port-based LBD, чтобы обнаружить петлю. При наличии на пути петли передаваемый пакет вернется на тот же порт или на другой порт того же устройства. При обнаружении портом, на котором включена функция LBD, петли, на порту будет отключена передача и получение пакетов.

Если включен режим VLAN-based, порт будет периодически отправлять пакеты VLAN-based LBD на каждую VLAN, членом которой является данный порт, и на которой включена функция LBD. Если порт является тегированным членом VLAN, будут отправлены тегированные пакеты LBD. Если порт является нетегированным членом VLAN, будут отправлены нетегированные пакеты LBD. При наличии на пути VLAN петли передача и получение пакетов будет временно остановлена на том порту закольцованной VLAN, где была обнаружена петля.

Если порт, на котором отключена функция LBD, получает пакет LBD и обнаруживает, что пакет отправлен системой, возможны два варианта: если тип данного пакета – port-based LBD, будет заблокирован порт отправления, а если тип пакета – VLAN-based LBD, будет заблокирована VLAN порта отправления.

Если на порту сконфигурирован режим VLAN-based, а порт является нетегированным членом нескольких VLAN, будет отправлен один нетегированный пакет LBD на каждую VLAN с указанием номера VLAN в поле VLAN пакета.

Восстановить порт, отключенный из-за ошибки, можно двумя способами: используйте команду **errdisable recovery cause loopback-detect**, чтобы включить автовосстановление, или восстановите порт вручную, применив сначала команду **shutdown**, а затем команду **no shutdown**.

Заблокированную VLAN можно восстановить автоматически, применив команду **errdisable recovery cause loopback-detect**. VLAN также можно восстановить вручную, применив сначала команду **shutdown**, а затем команду **no shutdown**.

Пример

В данном примере показано, как включить функцию LBD глобально и установить режим обнаружения port-based.

```
Switch#configure terminal
Switch(config)#loopback-detection
Switch(config)#loopback-detection mode port-based
Switch(config)#
```

41.2 loopback-detection (Interface)

Данная команда используется для включения функции LBD на интерфейсе. Для отключения данной функции на интерфейсе воспользуйтесь формой **no** этой команды.

loopback-detection
no loopback-detection

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и port-channel.

Используйте данную команду, чтобы включить/отключить функцию LBD на интерфейсе.

Пример

В данном примере показано, как включить функцию LBD на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#loopback-detection
Switch(config-if)#
```

41.3 loopback-detection interval

Данная команда используется для конфигурирования временного интервала. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

loopback-detection interval *SECONDS*
no loopback-detection interval

Параметры

SECONDS	Укажите интервал передачи пакетов LBD. Доступный диапазон значений: от 1 до 32767 секунд.

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы сконфигурировать интервал передачи пакетов LBD, отправляемых для обнаружения петли.

Пример

В данном примере показано, как сконфигурировать интервал 20 секунд.

```
Switch#configure terminal
Switch(config)#loopback-detection interval 20
Switch(config)#
```

41.4 loopback-detection vlan

Данная команда используется для того, чтобы включить функцию LBD на VLAN. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

loopback-detection vlan *VLAN-LIST*
no loopback-detection vlan *VLAN-LIST*

Параметры

VLAN-LIST	Укажите идентификационный номер / номера / диапазон номеров VLAN. Диапазоны разделяются при помощи дефисов. Значения разделяются при помощи запятых. Пробелы до и после дефиса/запятой недопустимы.

По умолчанию

По умолчанию данная опция включена для всех VLAN.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы сконфигурировать список VLAN, на которых включена функция LBD. Настройки команды будут применены, если на порту сконфигурирован режим обнаружения петли VLAN-based.

По умолчанию пакеты LBD Control отправляются на все VLAN, членом которых является данный порт. Пакеты LBD Control отправляются на VLAN, членом которых является данный порт из указанного списка VLAN.

Список VLAN можно расширить, применив команду несколько раз.

Пример

В данном примере показано, как включить функцию LBD в диапазоне с VLAN 100 по VLAN 200.

```
Switch#configure terminal
Switch(config)#loopback-detection vlan 100-200
Switch(config)#
```

41.5 show loopback-detection

Данная команда используется для отображения текущих настроек LBD.

show loopback-detection [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейс, который необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить настройки и статус функции LBD.

Пример

В данном примере показано, как отобразить текущие настройки и статус функции LBD.

```
Switch#show loopback-detection

 Loop Detection       : Disabled
 Detection Mode       : port-based
 LBD enabled VLAN     : all VLANs
 Interval             : 10 seconds
 Action Mode          : Shutdown
 Address Type         : Multicast
 Function Version     : v4.07

 Interface         State       Result               Time Left (sec)
 --------------    --------    -----------------    ---------------
 eth1/0/1          Disabled    Normal               -
 eth1/0/2          Disabled    Normal               -
 eth1/0/3          Disabled    Normal               -
 eth1/0/4          Disabled    Normal               -
 eth1/0/5          Disabled    Normal               -
 eth1/0/6          Disabled    Normal               -
 eth1/0/7          Disabled    Normal               -
 eth1/0/8          Disabled    Normal               -
 eth1/0/9          Disabled    Normal               -
 eth1/0/10         Disabled    Normal               -
 eth1/0/11         Disabled    Normal               -
 eth1/0/12         Disabled    Normal               -
 eth1/0/13         Disabled    Normal               -
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

В данном примере показано, как отобразить статус функции LBD для интерфейса Ethernet 1/0/1.

```
Switch# show loopback-detection interface eth1/0/1

Interface        State       Result               Time Left (sec)
-------------    --------    ------------------   ------------
eth1/0/1         Disabled    Normal               -

Switch#
```

Отображаемые параметры

Interface	Отображает порт, на котором включена функция LBD.
Status	Отображает статус порта.
Result	Отображает, обнаружена ли петля.
Time Left	Отображает время, оставшееся до автовосстановления.

41.6 loopback-detection action

Данная команда используется для настройки режима LBD. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

loopback-detection action {shutdown | none}

no loopback-detection action

Параметры

shutdown	Укажите, чтобы отключить порт в режиме port-based / заблокировать трафик на указанной VLAN в режиме VLAN-based при обнаружении петли.
none	Укажите, чтобы не отключать порт в режиме port-based / не блокировать трафик на указанной VLAN в режиме VLAN-based при обнаружении петли.

По умолчанию

Параметр по умолчанию – **shutdown**.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить режим LBD.

Пример

В данном примере показано, как настроить режим LBD.

```
Switch#configure terminal
Switch(config)#loopback-detection action none
Switch(config)#
```

41.7 snmp-server enable traps loopback-detection

Данная команда используется для включения отправки SNMP-уведомлений для LBD. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

snmp-server enable traps loopback-detection
no snmp-server enable traps loopback-detection

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы включить или отключить отправку SNMP-уведомлений для LBD.

Пример

В данном примере показано, как включить отправку SNMP-уведомлений для LBD.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps loopback-detection
Switch(config)#
```

41.8 loopback-detection address-type

Данная команда используется для того, чтобы настроить тип адреса назначения (destination) пакетов LBD. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

loopback-detection address-type {multicast | broadcast}
no loopback-detection address-type

Параметры

multicast	Укажите, чтобы отсылать только групповые пакеты LBD. Адрес назначения – CF-00-00-00-00-00.
broadcast	Укажите, чтобы отсылать только широковещательные пакеты LBD. Адрес назначения – FF-FF-FF-FF-FF-FF.

По умолчанию

Параметр по умолчанию – **multicast**.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить тип адреса назначения пакетов LBD.

Пример

В данном примере показано, как настроить тип адреса назначения пакетов LBD. Указанный тип – broadcast.

```
Switch#configure terminal
Switch(config)#loopback-detection address-type broadcast
Switch(config)#
```

42. Команды Mirror

42.1 monitor session destination interface

Данная команда используется, чтобы настроить интерфейс назначения (destination) для сессии мониторинга, позволяя отслеживать пакеты на портах источника (source) через порт назначения. Для удаления сессии мониторинга или интерфейса назначения сессии воспользуйтесь формой **no** этой команды.

monitor session *SESSION-NUMBER* **destination interface** *INTERFACE-ID*
no monitor session *SESSION-NUMBER* **destination interface** *INTERFACE-ID*
no monitor session *SESSION-NUMBER*

Параметры

session *SESSION-NUMBER*	Укажите номер сессии мониторинга. Доступный диапазон значений: от 1 до 4.
interface *INTERFACE-ID*	Укажите интерфейс назначения для сессии мониторинга.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить интерфейс назначения для локальной сессии мониторинга.

В качестве интерфейсов назначения для сессий мониторинга можно использовать физические порты и port-channel. Для сессии мониторинга можно указать несколько интерфейсов источника, но только один интерфейс назначения. Интерфейс не может быть одновременно интерфейсом источника одной сессии и портом назначения другой сессии. Интерфейс можно сконфигурировать в качестве интерфейса назначения нескольких сессий, но в качестве интерфейса источника только одной сессии.

Пример

В данном примере показано, как создать сессию мониторинга порта с номером 1, указав физический порт Ethernet 1/0/1 в качестве порта назначения, а три физических порта источника (от Ethernet 1/0/2 до Ethernet 1/0/4) в качестве портов источника.

```
Switch#configure terminal
Switch(config)#monitor session 1 destination interface eth1/0/1
Switch(config)#monitor session 1 source interface eth1/0/2-4
Switch(config)#
```

42.2 monitor session source interface

Данная команда используется, чтобы сконфигурировать порт источника (source) сессии мониторинга. Для удаления сессии мониторинга порта или порта источника из сессии мониторинга воспользуйтесь формой **no** этой команды.

monitor session *SESSION-NUMBER* **source interface** *INTERFACE-ID* **[, | -] [both | rx | tx]**
no monitor session *SESSION-NUMBER* **source interface** *INTERFACE-ID* **[, | -]**
no monitor session *SESSION-NUMBER*

Параметры

session *SESSION-NUMBER*	Укажите номер сессии мониторинга. Доступный диапазон: от 1 до 4.
interface *INTERFACE-ID*	Укажите интерфейс источника для сессии мониторинга.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
both	(Опционально.) Укажите, чтобы отслеживать пакеты, переданные и полученные портом.
rx	(Опционально.) Укажите, чтобы отслеживать пакеты, полученные портом.
tx	(Опционально.) Укажите, чтобы отслеживать пакеты, переданные портом.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

В качестве интерфейсов источника для сессий мониторинга можно использовать физические порты и port-channel.

Для сессии мониторинга можно указать несколько интерфейсов источника, но только один интерфейс назначения (destination). Интерфейс не может быть одновременно интерфейсом источника одной сессии и портом назначения другой сессии. Интерфейс можно сконфигурировать в качестве интерфейса назначения нескольких сессий, но в качестве интерфейса источника только одной сессии.

Если направление не указано или указан параметр **both**, отслеживается как переданный, так и полученный трафик.

Пример

В данном примере показано, как создать сессию мониторинга порта с номером 1. Физический порт Ethernet 1/0/1 указан в качестве порта назначения, а три физических порта источника (от Ethernet 1/0/2 до Ethernet 1/0/4) указаны в качестве портов источника.

```
Switch#configure terminal
Switch(config)#monitor session 1 destination interface eth1/0/1
Switch(config)#monitor session 1 source interface ethe1/0/2-4
Switch(config)#
```

42.3 show monitor session

Данная команда используется для отображения указанной сессии / всех сессий мониторинга.

show monitor session [*SESSION-NUMBER***]**

Параметры

SESSION-NUMBER	(Опционально.) Укажите номер сессии, которую необходимо отобразить. Доступный диапазон: от 1 до 4.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если не указаны дополнительные параметры, будут отображены все сессии мониторинга.

Пример

В данном примере показано, как отобразить сессию мониторинга порта с номером 1.

```
Switch#show monitor session

 Session 1
     Session Type: local session
     Destination Port: Ethernet1/0/1
     Source Ports:
         Both:
             Ethernet1/0/2
             Ethernet1/0/3
             Ethernet1/0/4

 Total Entries: 1

Switch#
```

43. Команды Multicast Listener Discovery (MLD) Snooping

43.1 clear ipv6 mld snooping statistics

Данная команда используется для обнуления счетчиков статистики MLD Snooping на коммутаторе.

clear ipv6 mld snooping statistics {all | vlan *VLAN-ID* **| interface** *INTERFACE-ID***}**

Параметры

all	Укажите, чтобы удалить статистику IPv6 MLD Snooping для всех VLAN и портов.
vlan *VLAN-ID*	Укажите необходимую VLAN.
interface *INTERFACE-ID*	Укажите необходимый интерфейс.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы обнулить счетчики статистики MLD Snooping на коммутаторе.

Пример

В данном примере показано, как удалить всю статистику MLD Snooping.

```
Switch#clear ipv6 mld snooping statistics all
Switch#
```

43.2 ipv6 mld snooping

Данная команда используется для включения MLD Snooping. Для отключения функции MLD Snooping воспользуйтесь формой **no** этой команды.

ipv6 mld snooping
no ipv6 mld snooping

Параметры

Нет.

По умолчанию

Функция MLD Snooping отключена на всех VLAN-интерфейсах.
Глобальное состояние MLD Snooping отключено.

Режим ввода команды

Global Configuration Mode.

VLAN Configuration Mode.

Использование команды

Чтобы применить MLD Snooping на VLAN, необходимо включить глобальное состояние MLD Snooping и MLD Snooping на VLAN. Настройки IGMP Snooping и MLD Snooping являются независимыми, поэтому их можно включать одновременно на одной и той же VLAN.

Пример

В примере ниже показано, как выключить MLD Snooping глобально.

```
Switch# configure terminal
Switch(config)# no ipv6 mld snooping
Switch(config)#
```

В примере ниже показано, как включить MLD Snooping глобально.

```
Switch#configure terminal
Switch(config)#ipv6 mld snooping
Switch(config)#
```

В следующем примере показано, как включить MLD Snooping на VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ipv6 mld snooping
Switch(config-vlan)#
```

43.3 ipv6 mld snooping fast-leave

Данная команда используется для включения функции MLD Snooping Fast Leave на VLAN. Для отключения данной опции воспользуйтесь формой **no** этой команды.

ipv6 mld snooping fast-leave
no ipv6 mld snooping fast-leave

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Используйте данную команду, чтобы удалить принадлежность MLD с порта сразу же после получения сообщения leave, не используя механизм запросов group-specific или group-and-source-specific query.

Пример

В данном примере показано, как включить функцию MLD Snooping Fast Leave на VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ipv6 mld snooping fast-leave
Switch(config-vlan)#
```

43.4 ipv6 mld snooping last-listener-query-interval

Данная команда используется для того, чтобы настроить интервал отправки сообщений group-specific или group-and-source-specific (channel) query. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld snooping last-listener-query-interval *SECONDS*

no ipv6 mld snooping last-listener-query-interval

Параметры

SECONDS	Укажите максимальный интервал между сообщениями group-specific query. В том числе учитываются сообщения, отправленные в ответ на сообщения leave-group. Диапазон значений: от 1 до 25.

По умолчанию

Значение по умолчанию – 1 секунда.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Получив сообщение done, MLD Snooping Querier считает, что на интерфейсе больше нет локальных участников, если после истечения времени ответа не пришло ни одно сообщение. Уменьшив данный интервал, можно сократить количество времени, которое требуется маршрутизатору для обнаружения потери последнего участника группы.

Пример

В данном примере показано, как настроить интервал last-listener-query на интерфейсе VLAN 1000. Указанное значение –3 секунды.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping last-listener-query-interval 3
Switch(config-vlan)#
```

43.5 ipv6 mld snooping mrouter

Данная команда используется для того, чтобы настроить указанный интерфейс в качестве IPv6 multicast router-порта или порта, которому запрещено подключаться к многоадресному маршрутизатору (forbidden), на интерфейсе VLAN. Для удаления интерфейса из списка multicast router-портов или портов, которым запрещено подключаться к многоадресному маршрутизатору (forbidden), воспользуйтесь формой **no** этой команды.

ipv6 mld snooping mrouter {interface *INTERFACE-ID* **[, | -] | forbidden interface** *INTERFACE-ID* **[, | -] | learn pimv6}**

no ipv6 mld snooping mrouter {interface *INTERFACE-ID* **[, | -] | forbidden interface** *INTERFACE-ID* **[, | -] | learn pimv6}**

Параметры

interface	Укажите диапазон интерфейсов, подключенных к многоадресным маршрутизаторам.
forbidden interface	Укажите диапазон интерфейсов, не подключенных к многоадресным маршрутизаторам.
INTERFACE-ID	Укажите интерфейс, который необходимо отобразить. Доступны физические интерфейсы или port-channel.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
learn pimv6	Укажите, чтобы включить динамическое изучение на портах, подключенных к многоадресному маршрутизатору.

По умолчанию

IPv6 multicast router-порт не настроен.
Автоматическое изучение включено.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

В качестве multicast router-порта можно использовать физический порт или port-channel. Указанный порт должен являться member-портом сконфигурированной VLAN.

Multicast router-порт может быть изучен динамически или сконфигурирован статически на устройстве с включенной функцией MLD Snooping. При динамическом изучении устройство MLD Snooping будет анализировать пакеты MLD и PIMv6, чтобы выяснить, является ли связанное устройство маршрутизатором.

Пример

В данном примере показано, как сконфигурировать интерфейс Ethernet 1/0/1 в качестве multicast router-порта с включенной функцией MLD Snooping, а интерфейс Ethernet 1/0/2 в качестве порта, которому запрещено подключаться к многоадресному маршрутизатору (forbidden) MLD Snooping, на VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ipv6 mld snooping mrouter interface eth1/0/1
Switch(config-vlan)#ipv6 mld snooping mrouter forbidden interface eth1/0/2
Switch(config-vlan)#
```

В данном примере показано, как отключить автоматическое изучение пакетов протокола маршрутизации на VLAN 4.

```
Switch#configure terminal
Switch(config)#vlan 4
Switch(config-vlan)#no ipv6 mld snooping mrouter learn pimv6
Switch(config-vlan)#
```

43.6 ipv6 mld snooping querier

Данная команда используется для включения MLD Snooping Querier на коммутаторе. Для отключения MLD Snooping Querier воспользуйтесь формой **no** этой команды.

ipv6 mld snooping querier
no ipv6 mld snooping querier

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Если система может выполнить роль Querier, устройство будет анализировать пакеты MLD query, отправленные другими устройствами. При получении сообщения MLD query устройство с меньшим значением IPv6-адреса становится Querier.

Пример

В данном примере показано, как включить состояние MLD Snooping Querier на VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ipv6 mld snooping querier
Switch(config-vlan)#
```

43.7 ipv6 mld snooping query-interval

Данная команда используется для того, чтобы задать интервал отправки сообщений MLD general query. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld snooping query-interval *SECONDS*

no ipv6 mld snooping query-interval

Параметры

SECONDS	Укажите интервал между сообщениями MLD general query, которые отправляет указанный маршрутизатор. Диапазон значений: от 1 до 31744.

По умолчанию

Значение по умолчанию – 125 секунд.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Query interval – это промежуток времени между запросами general query, отправляемыми Querier. Изменяя данный интервал, можно настроить количество сообщений MLD в сети. Чем больше значение интервала, тем реже будут отправляться сообщения MLD query.

Пример

В данном примере показано, как настроить интервал MLD snooping query на VLAN 1000. Указанное значение – 300 секунд.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping query-interval 300
Switch(config-vlan)#
```

43.8 ipv6 mld snooping query-max-response-time

Данная команда используется для настройки максимального времени ответа, анонсированного в запросах MLD snooping query. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld snooping query-max-response-time *SECONDS*

no ipv6 mld snooping query-max-response-time

Параметры

SECONDS	Укажите максимальное время ответа, анонсированное в сообщениях MLD snooping query. Диапазон значений: от 1 до 25 секунд.

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Команда применяется для настройки периода времени, в течение которого участник группы может ответить на сообщение MLD query. После истечения данного периода его принадлежность к группе будет удалена.

Пример

В данном примере показано, как настроить максимальное время ответа на VLAN 1000. Указанное значение – 20 секунд.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping query-max-response-time 20
Switch(config-vlan)#
```

43.9 ipv6 mld snooping query-version

Данная команда используется для того, чтобы настроить версию пакетов general query, отправленного MLD Snooping Querier. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld snooping query-version *NUMBER*
no ipv6 mld snooping query-version

Параметры

NUMBER	Укажите версию пакета MLD general query, отправленного MLD Snooping Querier (1 или 2).

По умолчанию

Версия по умолчанию – 2.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить версию пакета MLD general query, отправленного MLD Snooping Querier.

Пример

В данном примере показано, как указать версию query на VLAN 1000. Указанная версия – 1.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping query-version 1
Switch(config-vlan)#
```

43.10 ipv6 mld snooping report-suppression

Данная команда используется для включения функции MLD Report Suppression на VLAN. Для отключения MLD Report Suppression на VLAN воспользуйтесь формой **no** этой команды.

ipv6 mld snooping report-suppression
no ipv6 mld snooping report-suppression

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Функция Report Suppression работает только для трафика MLDv1.

Если функция Report Suppression включена, коммутатор блокирует дублированные сообщения, отправленные узлами. Дублированные сообщения report или leave для одной группы будут блокироваться до тех пор, пока не истечет время блокировки. Будет передано только одно сообщение report или leave, остальные сообщения будут заблокированы.

Пример

В данном примере показано, как включить функцию MLD Report Suppression.

```
Switch#configure terminal
Switch(config)#vlan 100
Switch(config-vlan)#ipv6 mld snooping report-suppression
Switch(config-vlan)#
```

43.11 ipv6 mld snooping robustness-variable

Данная команда используется для настройки значения robustness variable для MLD Snooping. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld snooping robustness-variable *VALUE*
no ipv6 mld snooping robustness-variable

Параметры

VALUE	Укажите значение robustness variable в диапазоне от 1 до 7.

По умолчанию

Значение по умолчанию – 2.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Robustness variable обеспечивает точную настройку в соответствии с ожидаемой потерей пакетов на интерфейсе. Значение robustness variable используется для вычисления следующих интервалов сообщений MLD:

- **Group member interval** – промежуток времени, по истечении которого маршрутизатор считает, что в группе больше нет активных участников. Данный интервал рассчитывается следующим образом: (robustness variable x query interval) + (1 x query response interval).
- **Other querier present interval** – промежуток времени, по истечении которого многоадресный маршрутизатор считает, что маршрутизатор, являющийся Querier, больше не доступен. Данный интервал рассчитывается следующим образом: (robustness variable x query interval) + (0,5 x query response interval).
- **Last member query count** – количество запросов group-specific query, отправленных маршрутизатором до того, как он предполагает, что в группе нет локальных участников. Количество по умолчанию равно значению robustness variable.

Данное значение может быть увеличено, если в подсети ожидается потеря пакетов.

Пример

В данном примере показано, как сконфигурировать значение robustness variable на VLAN 1000. Указанное значение – 3.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping robustness-variable 3
Switch(config-vlan)#
```

43.12 ipv6 mld snooping static-group

Данная команда используется для настройки статической группы MLD Snooping. Для удаления статической группы воспользуйтесь формой **no** этой команды.

ipv6 mld snooping static-group *IPV6-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**

no ipv6 mld snooping static-group *IPV6-ADDRESS* **[interface** *INTERFACE-ID* **[, | -]]**

Параметры

IPV6-ADDRESS	Укажите IPv6-адрес многоадресной группы.
interface *INTERFACE-ID*	Укажите интерфейс, который необходимо использовать. Доступны физические интерфейсы или port-channel.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию статическая группа не сконфигурирована.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Используйте данную команду на интерфейсе VLAN, чтобы добавить статические записи о принадлежности к группе.

Используйте данную команду, чтобы создать статическую группу MLD Snooping, если прикрепленный узел не поддерживает протокол MLD.

Пример

В данном примере показано, как статически добавить группу для MLD Snooping на VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ipv6 mld snooping static-group FF02::12:03 interface eth1/0/5
Switch(config-vlan)#
```

43.13 ipv6 mld snooping suppression-time

Данная команда используется для настройки времени блокирования дублированных сообщений MLD report или MLD leave. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld snooping suppression-time *SECONDS*

no ipv6 mld snooping suppression-time

Параметры

SECONDS	Укажите, чтобы настроить время блокирования дублированных сообщений MLD report. Диапазон значений: от 1 до 300.

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Функция Report Suppression будет блокировать дублированные пакеты MLD report или MLD leave, полученные в течение времени блокирования. Чем меньше время блокирования, тем чаще будут отправляться дублированнные пакеты MLD.

Пример

В данном примере показано, как настроить время блокирования на VLAN 1000. Указанное значение – 125.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping suppression-time 125
Switch(config-vlan)#
```

43.14 ipv6 mld snooping minimum-version

Данная команда используется для настройки минимальной версии MLD, разрешенной на VLAN. Для удаления заданного ограничения воспользуйтесь формой **no** этой команды.

ipv6 mld snooping minimum-version 2

no ipv6 mld snooping minimum-version

Параметры

Нет.

По умолчанию

По умолчанию ограничение не установлено.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Данные настройки применимы только для фильтрации сообщений об участии MLD.

Пример

В данном примере показано, как ограничить подключение к VLAN 1 всех узлов MLDv1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ipv6 mld snooping minimum-version 2
Switch(config-vlan)#
```

43.15 show ipv6 mld snooping

Данная команда используется для отображения информации об MLD Snooping на коммутаторе.

show ipv6 mld snooping [vlan *VLAN-ID***]**

Параметры

vlan *VLAN-ID*	(Опционально.) Укажите VLAN для отображения.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если параметры не указаны, будет отображена информация об MLD Snooping для всех VLAN, на которых включена данная функция.

Пример

В данном примере показано, как отобразить настройки MLD Snooping.

```
Switch#show ipv6 mld snooping

MLD snooping global state: Enabled

VLAN #1 configuration
    MLD snooping state           : Enabled
    Minimum version              : v1
    Fast leave                   : Disabled (port-based)
    Report suppression           : Disabled
    Suppression time             : 10 seconds
    Mrouter port learning        : Enabled
    Querier state                : Disabled
    Query version                : v2
    Query interval               : 125 seconds
    Max response time            : 10 seconds
    Robustness value             : 2
    Last listener query interval : 1 seconds

Total Entries: 1

Switch#
```

43.16 show ipv6 mld snooping groups

Данная команда используется для отображения информации о группах MLD Snooping, изученных на коммутаторе.

show ipv6 mld snooping groups [*IPV6-ADDRESS* **| vlan** *VLAN-ID***] [detail]**

Параметры

IPV6-ADDRESS	(Опционально.) Укажите IP-адрес группы. Если IPv6-адрес не указан, будет отображена информация обо всех группах MLD Snooping.
vlan *VLAN-ID*	(Опционально.) Укажите VLAN ID для отображения. Если VLAN не указана, будет отображена информация о группе MLD Snooping для всех VLAN.

,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
detail	(Опционально.) Укажите, чтобы отобразить подробную информацию о группе MLD Snooping.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить информацию о группе MLD Snooping.

Пример

В данном примере показано, как отобразить информацию о группе MLD Snooping.

```
Switch#show ipv6 mld snooping groups

Total Group Entries : 1
Total Source Entries: 1

vlan1, FF1E::1
Learned on port: 1/0/3

Switch#
```

В данном примере показано, как отобразить подробную информацию о группе MLD Snooping.

```
Switch# show ipv6 mld snooping groups detail

Total Group Entries : 1
Total Source Entries: 1

vlan1, FF1E::1
Learned on port: 1/0/3
  1/0/3
    version: v2, filter mode: Include, uptime: 0DT00H00M09S, expires: 0DT00H00M00S
      source 2000::1, uptime: 0DT00H00M09S, expires: 0DT00H04M11S

Switch#
```

43.17 show ipv6 mld snooping mrouter

Данная команда используется для отображения информации об автоматически изученном или настроенном вручную многоадресном маршрутизаторе MLD Snooping.

show ipv6 mld snooping mrouter [vlan *VLAN-ID* **[, | -]]**

Параметры

vlan *VLAN-ID*	(Опционально.) Укажите VLAN ID для отображения. Если VLAN не указана, будет отображена информация о многоадресном маршрутизаторе MLD Snooping на всех VLAN.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить интерфейсы динамически изученного или настроенного вручную многоадресного маршрутизатора.

Пример

В данном примере показано, как отобразить информацию о многоадресном маршрутизаторе MLD Snooping.

```
Switch#show ipv6 mld snooping mrouter

VLAN    Ports
-----   ----------------------------
1       eth1/0/4 (static)
        eth1/0/2 (forbidden)

Total Entries: 1

Switch#
```

43.18 show ipv6 mld snooping static-group

Данная команда используется для отображения статически настроенной группы MLD Snooping на коммутаторе.

show ipv6 mld snooping static-group [*GROUP-ADDRESS* **| vlan** *VLAN-ID***]**

Параметры

GROUP-ADDRESS	(Опционально.) Укажите IPv6-адрес группы для отображения.
vlan *VLAN-ID*	(Опционально.) Укажите VLAN ID для отображения.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить статически настроенную группу MLD Snooping.

Пример

В данном примере показано, как отобразить статически настроенную группу MLD Snooping.

```
Switch#show ipv6 mld snooping static-group

VLAN ID Group address                          Interface
------- ------------------------------------- ------------------
1       FF1E::1                                eth1/0/6

Total Entries: 1

Switch#
```

43.19 show ipv6 mld snooping statistics

Данная команда используется для отображения статистики MLD Snooping на коммутаторе.

show ipv6 mld snooping statistics {interface [*INTERFACE-ID***[, | -]] | vlan [***VLAN-ID* **[, | -]]}**

Параметры

interface	Укажите, чтобы отобразить счетчики статистики для интерфейса.
INTERFACE-ID	(Опционально.) Укажите интерфейсы для отображения.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
vlan	Укажите, чтобы отобразить счетчики статистики для VLAN.
VLAN-ID	(Опционально.) Укажите VLAN ID для отображения.

,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить статистику MLD Snooping.

Пример

В данном примере показано, как отобразить статистику MLD Snooping для интерфейса Ethernet 1/0/4.

```
Switch# show ipv6 mld snooping statistics interface eth1/0/4

Interface eth1/0/4
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Total Entries: 1

Switch#
```

В данном примере показано, как отобразить статистику MLD Snooping для VLAN 1.

```
Switch# show ipv6 mld snooping statistics vlan 1
VLAN 1 Statistics:
  Rx: V1Report 3, v2Report 0, Query 3, v1Done 0
  Tx: v1Report 2, v2Report 2, Query 1, v1Done 2

Total Entries: 1
Switch#
```

44. Команды Multiple Spanning Tree Protocol (MSTP)

44.1 instance

Данная команда используется для сопоставления VLAN с экземпляром MST (Multiple Spanning Tree). Для удаления указанного экземпляра MST воспользуйтесь командой **no instance** *INSTANCE-ID*. Для возврата VLAN к экземпляру по умолчанию (CIST) воспользуйтесь командой **no instance** *INSTANCE-ID* **vlans** *VLAND-ID* **[, | -]**.

instance *INSTANCE-ID* **vlans** *VLAN-ID* **[, | -]**
no instance *INSTANCE-ID* **[vlans** *VLAN-ID* **[, | -]]**

Параметры

INSTANCE-ID	Укажите идентификатор экземпляра MSTP, к которому необходимо привязать указанные VLAN. Диапазон значений: от 1 до 32.
vlans *VLAN-ID*	Укажите VLAN, которые необходимо привязать или удалить из указанного экземпляра. Диапазон значений: от 1 до 4094.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

MST Configuration Mode.

Использование команды

Любая непривязанная VLAN привязывается к экземпляру CIST. Во время привязки VLAN к несуществующему экземпляру, экземпляр будет создан автоматически. Если все VLAN экземпляра удалены, экземпляр будет удален автоматически. Пользователи могут удалить экземпляр вручную, используя команду **no instance** без указания VLAN.

Пример

В данном примере показано, как привязать несколько VLAN к экземпляру 2.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance 2 vlans 1-100
Switch(config-mst)#
```

44.2 name

Данная команда используется для настройки имени региона MST (MST region). Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

name *NAME*
no name *NAME*

Параметры

NAME	Укажите имя региона MST. Максимальное количество символов – 32. Тип – общая строка, допускающая пробелы.

По умолчанию

Имя по умолчанию – MAC-адрес коммутатора.

Режим ввода команды

MST Configuration Mode.

Использование команды

Если у коммутаторов совпадают VLAN Mapping и номер версии конфигурации, но различаются имена регионов, они принадлежат к разным MST-регионам.

Пример

В примере показано, как настроить имя региона MST – «MName».

```
Switch#configure terminal
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# name MName
Switch(config-mst)#
```

44.3 revision

Данная команда используется, чтобы указать номер ревизии для конфигурации MST. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

revision *VERSION*
no revision

Параметры

VERSION	Укажите номер ревизии для MST. Диапазон значений: от 0 до 65535.

По умолчанию

Значение по умолчанию – 0.

Режим ввода команды

MST Configuration Mode.

Использование команды

Данная команда применяется, чтобы указать номер ревизии для конфигурации MST. При наличии более одного коммутатора с одинаковыми настройками, но с различными ревизиями, считается, что данные коммутаторы находятся в разных регионах MST.

Пример

В данном примере показано, как указать ревизию «2» для конфигурации MST.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#revision 2
Switch(config-mst)#
```

44.4 show spanning-tree mst

Данная команда используется для отображения информации, которая использовалась в версии MSTP.

show spanning-tree mst [configuration [digest]]

show spanning-tree mst [instance *INSTANCE-ID* **[, | -]] [interface** *INTERFACE-ID* **[, | -]] [detail]**

Параметры

configuration	(Опционально.) Укажите для отображения текущей конфигурации MST оборудования.
digest	(Опционально.) Укажите для отображения MD5 digest, включенного в идентификатор настройки текущего MST (MSTCI).
instance *INSTANCE-ID*	(Опционально.) Укажите номер экземпляра для отображения.
,	(Опционально.) Используется для перечисления нескольких экземпляров или отделения одного диапазона экземпляров от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона экземпляров. Пробелы до и после дефиса недопустимы.
interface *INTERFACE-ID*	(Опционально.) Укажите ID интерфейса для отображения.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду для отображения настроек и рабочего состояния MSTP. Если настроена Private VLAN, а второстепенная (Secondary) VLAN не привязана к той же основной (Primary) VLAN, команда **show spanning-tree mst configuration** отобразит сообщение, указывающее на это условие.

Пример

В данном примере показано, как отобразить подробную информацию об MSTP.

```
Switch#show spanning-tree mst detail

 Spanning tree: Disabled,protocol: RSTP
 Number of MST instances: 1

 >>>>MST00  vlans mapped : 1-4094
 Bridge address: F0-7D-68-12-10-01, priority: 32768 (32768 sysid 0)
 Designated root address: 00-00-00-00-00-00, priority: 0 (0 sysid 0)
 CIST  external root cost : 0
 Regional root bridge address: 00-00-00-00-00-00, priority: 0 (0 sysid 0)
 CIST  internal root cost : 0
 Designated bridge address: 00-00-00-00-00-00, priority: 0 (0 sysid 0)
 Topology changes count: 0

 eth1/0/1
   Port state: forwarding
   Port role: nonStp
   Port info : port id 128.1, priority: 128, cost: 200000
   Designated root address: 00-00-00-00-00-00, priority: 0
   Regional root address: 00-00-00-00-00-00, priority: 0
   Designated bridge address: 00-00-00-00-00-00, priority: 0, port id: 0.0

 eth1/0/3
   Port state: forwarding
   Port role: nonStp
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

В данном примере показано, как отобразить подробную информацию об MSTP для интерфейса eth1/0/1.

```
Switch# show spanning-tree mst interface eth1/0/1 detail

eth1/0/1
 Configured link type: auto, operation status: point-to-point
 Configured fast-forwarding: auto, operation status: non-edge
 Bpdu statistic counter: sent: 0, received: 0

 >>>>MST instance: 00,  vlans mapped : 1-4094
 Port state: forwarding
 Port role: nonStp
 Port info : port ID 128.1, priority: 128, cost: 200000
 Designated root address: 00-00-00-00-00-00, priority: 0
 Regional Root address: 00-00-00-00-00-00, priority: 0
 Designated bridge address: 00-00-00-00-00-00, priority: 0, port id: 0.0


Switch#
```

В данном примере показано, как отобразить краткую информацию об MSTP.

```
S Switch#show spanning-tree mst

 Spanning tree: Disabled,protocol: RSTP
 Number of MST instances: 1

 >>>>MST00  vlans mapped : 1-4094
 Bridge address: F0-7D-68-12-10-01, priority: 32768 (32768 sysid 0)
 Designated root address: 00-00-00-00-00-00, priority: 0 (0 sysid 0)
 CIST  external root cost : 0
 Regional root bridge address: 00-00-00-00-00-00, priority: 0 (0 sysid 0)
 CIST  internal root cost : 0
 Designated bridge address: 00-00-00-00-00-00, priority: 0 (0 sysid 0)
 Topology changes count: 0

                                          Priority Link
 Interface      Role       State      Cost      .Port#   Type   Edge
 ---------      ----       -----      ----      -------  -----  ----
 eth1/0/1       nonStp     forwarding 200000    128.1    p2p    non-edge
 eth1/0/3       nonStp     forwarding 200000    128.3    p2p    non-edge


Switch#
```

В данном примере показано, как отобразить краткую информацию об MSTP для интерфейсов от eth1/0/3 до eth1/0/4.

```
Switch# show spanning-tree mst interface eth1/0/3-4

eth1/0/3
 Configured link type: auto, operation status: point-to-point
 Configured fast-forwarding: auto, operation status: edge
 Bpdu statistic counter: sent: 4, received: 0

                                          Priority
 Instance Role       State      Cost      .Port#
 -------- ---------- ---------- --------- ---------
 MST00    designated forwarding 20000     128.3
 MST01    backup     blocking   200000    128.3

eth1/0/4
 Configured link type: auto, operation status: point-to-point
 Configured fast-forwarding: auto, operation status: edge
 Bpdu statistic counter: sent: 4, received: 0

                                          Priority
 Instance Role       State      Cost      .Port#
 -------- ---------- ---------- --------- ---------
 MST00    root       forwarding 20000     128.4
 MST01    backup     blocking   200000    128.4

Switch#
```

В данном примере показано, как отобразить краткую информацию об MSTP для интерфейсов от eth1/0/3 до eth1/0/4 MST02.

```
Switch# show spanning-tree mst instance 2 interface eth1/0/3-4

 >>>>MST02 vlans mapped : 2-3
 Bridge Address: 00-12-d9-87-47-00 , Priority: 32770 (32768 sysid 2)
 Designated Root Address: 00-12-d9-87-47-00 , Priority: 32770
 Designated Bridge Address: 00-12-d9-87-47-00 , Priority: 32770
 Topology Changes Count: 0

                                              Priority Link
 Interface      Role       State      Cost      .Port#   Type   Edge
 ---------      ----       -----      ----      -------  -----  ----
 eth1/0/3       backup     blocking   200000    128.3    p2p    non-edge
 eth1/0/4       backup     blocking   200000    128.4    p2p    non-edge

Switch#
```

В данном примере показано, как отобразить настройки привязки экземпляра MSTP.

```
Switch# show spanning-tree mst configuration

 Name      : MName
 Revision : 2,Instances configured: 3
 Instance    Vlans
 -------     ------------------------------------------------------------
       0     21-4094
       1     1-10
       2     11-20

Switch#
```

44.5 spanning-tree mst

Данная команда позволяет настроить стоимость пути и приоритет порта для экземпляра MST. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

spanning-tree mst *INSTANCE-ID* **{cost** *COST* **| port-priority** *PRIORITY***}**
no spanning-tree mst *INSTANCE-ID* **{cost | port-priority}**

Параметры

INSTANCE-ID	Укажите идентификатор экземпляра MSTP.
cost *COST*	Укажите стоимость пути экземпляра. Диапазон значений: от 1 до 200000000.
port-priority *PRIORITY*	Укажите приоритет порта экземпляра. Диапазон значений: от 0 до 240 с шагом 16.

По умолчанию

Стоимость указывается на основе скорости порта. Чем выше скорость, тем меньше стоимость пути. MST всегда использует стоимость «длинного» пути (long path cost).
Приоритет порта – 128.

Режим ввода команды

Interface Configuration Mode.

Использование команды

При вводе стоимости запятая в записи не ставится. Пример верного варианта: 1000. Пример неверного варианта: 1,000.

Пример

В данном примере показано, как настроить стоимость пути интерфейса eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# spanning-tree mst 0 cost 17031970
Switch(config-if)#
```

44.6 spanning-tree mst configuration

Данная команда используется для входа в режим MST Configuration. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

spanning-tree mst configuration
no spanning-tree mst configuration

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда применяется для входа в режим MST Configuration Mode.

Пример

В данном примере показано, как войти в режим MST Configuration Mode.

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

44.7 spanning-tree mst max-hops

Данная команда используется, чтобы указать максимальное число переходов для служебных пакетов MSTP. Для возврата к настройками по умолчанию воспользуйтесь формой **no** этой команды.

spanning-tree mst max-hops *HOP-COUNT*
no spanning-tree mst max-hops

Параметры

max-hops *HOP-COUNT*	Укажите максимальное число переходов для служебных пакетов MSTP. Диапазон значений: от 1 до 40.

По умолчанию

Значение по умолчанию – 20.

Режим ввода команды

Global Configuration Mode.

Использование команды

Команда применяется, чтобы указать максимальное число переходов для служебных пакетов MSTP.

Пример

В данном примере показано, как указать максимальное число переходов для служебных пакетов MSTP.

```
Switch#configure terminal
Switch(config)#spanning-tree mst max-hops 19
Switch(config)#
```

44.8 spanning-tree mst hello-time

Данная команда применяется, чтобы указать интервал отправки hello-сообщений, используемых в версии MSTP для определенного порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

spanning-tree mst hello-time *SECONDS*
no spanning-tree mst hello-time

Параметры

SECONDS	Укажите интервал отправки одного BPDU на указанном порту. Диапазон значений: от 1 до 2 секунд.

По умолчанию

По умолчанию интервал отправки hello-сообщений – 2 секунды.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда действует только в режиме MSTP.

Пример

В данном примере показано, как указать интервал отправки hello-сообщений, используемых в версии MSTP, на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# spanning-tree mst hello-time 1
Switch(config-if)#
```

44.9 spanning-tree mst priority

Данная команда используется для настройки значения приоритета моста для выбранного MSTP-экземпляра. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

spanning-tree mst *INSTANCE-ID* **priority** *PRIORITY*
no spanning-tree mst *INSTANCE-ID* **priority**

Параметры

INSTANCE-ID	Укажите идентификатор экземпляра MSTP. Экземпляр 0 − это экземпляр по умолчанию, CIST.
PRIORITY	Укажите приоритет моста, значение которого должно делиться на 4096. Доступный диапазон значений: от 0 до 61440.

По умолчанию

Значение по умолчанию – 32768.

Режим ввода команды

Global Configuration Mode.

Использование команды

Приоритет имеет то же значение, что и приоритет моста в справочнике команд STP, но можно указать другое значение приоритета для разных экземпляров MSTP.

Пример

В данном примере показано, как указать приоритет моста для экземпляра MSTP 2.

```
Switch#configure terminal
Switch(config)#spanning-tree mst 2 priority 0
Switch(config)#
```

45. Команды Neighbor Discovery (ND) Inspection

45.1 ipv6 nd inspection policy

Данная команда используется для создания политики ND Inspection Policy и для входа в режим ND Inspection Policy Configuration Mode. Чтобы удалить политику ND Inspection Policy, воспользуйтесь формой **no** этой команды.

ipv6 nd inspection policy *POLICY-NAME*
no ipv6 nd inspection policy *POLICY-NAME*

Параметры

POLICY-NAME	Укажите имя политики ND Inspection Policy.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы создать политику ND Inspection Policy и войти в режим ND Inspection Policy Configuration Mode. ND Inspection предназначена для проверки сообщений Neighbor Solicitation (NS) и Neighbor Advertisement (NA).

Пример

В данном примере показано, как создать политику ND под именем «policy1».

```
Switch#configure terminal
Switch(config)#ipv6 nd inspection policy policy1
Switch(config-nd-inspection)#
```

45.2 validate source-mac

Данная команда используется для проверки MAC-адреса на соответствие адресу Link Layer для ND-сообщений. Чтобы отменить проверку, воспользуйтесь формой **no** этой команды.

validate source-mac
no validate source-mac

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

ND Inspection Policy Configuration Mode.

Использование команды

Когда на коммутаторе будет получено ND-сообщение, содержащее адрес Link Layer, исходный MAC-адрес будет проверен на соответствие данному адресу Link Layer. При несовпадении адреса Link Layer и MAC-адреса пакет будет отброшен.

Пример

В данном примере показано, как настроить на коммутаторе действие отбрасывания для ND-сообщения, адрес Link Layer которого не соответствует MAC-адресу.

```
Switch#configure terminal
Switch(config)#ipv6 nd inspection policy policy1
Switch(config-nd-inspection)#validate source-mac
Switch(config-nd-inspection)#
```

45.3 device-role

Данная команда используется для указания роли подключенного устройства. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

device-role {host | router}

no device-role

Параметры

host	Укажите, чтобы настроить устройство в качестве узла.
router	Укажите, чтобы настроить устройство в качестве маршрутизатора.

По умолчанию

Роль устройства по умолчанию – host.

Режим ввода команды

ND Inspection Policy Configuration Mode.

Использование команды

Используйте данную команду, чтобы указать роль подключенного устройства. Так как по умолчанию устройство выполняет роль узла (host), проверка сообщений NS и NA выполняется. Если устройство настроено в качестве маршрутизатора (router), проверка сообщений NS и NA не выполняется. Сообщения NS и NA проверяются в соответствии с таблицей динамической привязки, информация о которой была получена из протокола ND или DHCP.

Пример

В данном примере показано, как создать политику ND под именем «policy1» и настроить устройство в качестве узла (host).

```
Switch#configure terminal
Switch(config)#ipv6 nd inspection policy policy1
Switch(config-nd-inspection)#device-role host
Switch(config-nd-inspection)#
```

45.4 ipv6 nd inspection attach-policy

Данная команда используется для применения политики ND Inspection Policy на определенном интерфейсе. Чтобы удалить политику ND Inspection Policy, воспользуйтесь формой **no** этой команды.

ipv6 nd inspection attach-policy [*POLICY-NAME***]**
no ipv6 nd inspection attach-policy

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики ND Inspection Policy.

По умолчанию

По умолчанию политика ND Inspection Policy не применена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.

Используйте данную команду, чтобы применить политику ND Inspection Policy на определенном интерфейсе. Если указан параметр **no**, для политики по умолчанию действуют следующие правила:

Сообщения NS/NA проверяются.

MAC-адрес источника в заголовке пакета уровня 2 не проверяется.

Пример

В данном примере показано, как применить политику ND Inspection Policy под именем «policy1» на интерфейсе Ethernet 1/0/3.

```
Switch#configure terminal
Switch(config)#ipv6 nd inspection policy policy1
Switch(config-nd-inspection)#device-role host
Switch(config-nd-inspection)#validate source-mac
Switch(config-nd-inspection)#exit
Switch(config)#interface eth1/0/3
Switch(config-if)#ipv6 nd inspection attach-policy policy1
Switch(config-if)#
```

45.6 show ipv6 nd inspection policy

Данная команда используется для отображения информации о политике ND Inspection Policy.

show ipv6 nd inspection policy [*POLICY-NAME***]**

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики ND Inspection Policy.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить информацию о политике ND Inspection Policy. Если параметр не указан, отображаться будет информация для всех политик.

Пример

В данном примере показано, как отобразить конфигурацию политики под именем «inspect1».

```
Switch#show ipv6 nd inspection policy inspect1

Policy inspect1 configuration:
   Device Role: host
   Validate Source MAC: Enabled
   Target: eth1/0/1-1/0/2

Switch#
```

46. Команды Network Access Authentication

46.1 authentication guest-vlan

Данная команда используется для настройки Guest VLAN. Чтобы удалить Guest VLAN, воспользуйтесь формой **no** этой команды.

authentication guest-vlan *VLAN-ID*
no authentication guest-vlan

Параметры

VLAN-ID	Укажите Guest VLAN для аутентификации.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Команда не может быть использована, если указанная VLAN не существует в качестве статической VLAN. Узел не может получить доступ к сети, пока не пройдет аутентификацию. Если Guest VLAN настроена, узлу разрешается доступ только к Guest VLAN без прохождения аутентификации. Во время аутентификации, если RADIUS-сервер назначает пользователю VLAN, пользователь будет авторизован в назначенной VLAN. Назначение Guest VLAN и VLAN не действует на порт trunk VLAN и порт tunnel VLAN.

Обычно назначение Guest VLAN и VLAN действует для узлов, подключенных к нетегированным портам. Данный функционал не применим в случае, если узлы обмениваются тегированным трафиком.

Если режим узла (host mode) аутентификации настроен как **multi-host**, порт будет добавлен как Guest VLAN порт, а PVID порта будет изменен на Guest VLAN. Трафик, приходящий из Guest VLAN, будет перенаправлен независимо от аутентификации. Трафик, приходящий от других VLAN, будет отбрасываться, пока не пройдет аутентификацию. Когда один узел проходит аутентификацию, порт покидает Guest VLAN и будет добавлен в назначенную VLAN. PVID порта будет изменен на назначенную VLAN.

Если режим узла (host mode) аутентификации настроен как **multi-auth**, порт будет добавлен как Guest VLAN порт, и PVID порта будет изменен на Guest VLAN. Узлам, которым разрешен доступ к Guest VLAN, запрещен доступ к другим VLAN, пока они не пройдут аутентификацию. Если один узел проходит аутентификацию, порт останется в Guest VLAN, а PVID порта не будет изменен.

Если Guest VLAN отключена, порт выйдет из Guest VLAN и вернется к родной VLAN (native). PVID изменится на PVID родной VLAN.

Пример

В данном примере показано, как указать VLAN 5 в качестве Guest VLAN.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication guest-vlan 5
Switch(config-if)#
```

46.2 authentication host-mode

Данная команда используется для указания режима аутентификации. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

authentication host-mode {multi-host | multi-auth}

no authentication host-mode

Параметры

multi-host	Укажите порт для работы в режиме multi-host. Выполняется только одна аутентификация, и все хосты, подключенные к порту, будут разрешены.
multi-auth	Укажите порт для работы в режиме multi-auth. Каждый узел будет проходить аутентификацию индивидуально.

По умолчанию

По умолчанию используется **multi-auth**.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Если порт работает в режиме **multi-host** и аутентифицирован один из узлов, всем другим узлам будет разрешен доступ к порту. Согласно аутентификации 802.1X, если повторная аутентификация завершается неудачно или аутентифицированный пользователь выходит из учетной записи, порт будет блокироваться на период молчания (quiet period). Порт восстановит обработку пакетов EAPOL после периода молчания.

Если порт работает в режиме **multi-auth**, каждый узел должен проходить аутентификацию индивидуально для доступа к порту. Узел представлен своим MAC-адресом. Доступ есть только у авторизованных узлов.

Пример

В данном примере показано, как назначить режим multi-host для интерфейса Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication host-mode multi-host
Switch(config-if)#
```

46.3 authentication periodic

Данная команда используется для включения периодического повторения аутентификации для порта. Для отключения периодического повторения аутентификации воспользуйтесь формой **no** этой команды.

authentication periodic
no authentication periodic

Параметры

Нет.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Используйте команду для включения/отключения периодического повторения аутентификации для порта.

Пример

В данном примере показано, как включить периодическое повторение аутентификации для интерфейса Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication periodic
Switch(config-if)#
```

46.4 authentication timer reauthentication

Данная команда используется для настройки таймера, по истечении которого будет необходимо пройти повторную аутентификацию. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

authentication timer reauthentication {*SECONDS***}**
no authentication timer reauthentication

Параметры

SECONDS	Укажите время, по истечении которого будет необходимо пройти повторную аутентификацию. Диапазон значений: от 1 до 65535.

По умолчанию

Значение по умолчанию – 3600 секунд.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Команда используется для настройки таймера, по истечении которого будет необходимо пройти повторную аутентификацию.

Пример

В данном примере показано, как настроить значение таймера повторной аутентификации для интерфейса Ethernet 1/0/1. Указанное значение – 200.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication timer reauthentication 200
Switch(config-if)#
```

46.5 authentication timer restart

Данная команда используется для настройки таймера, по истечении которого станет возможна повторная аутентификация после последней неудачной попытки. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

authentication timer restart *SECONDS*

no authentication timer restart

Параметры

SECONDS	Укажите время, по истечении которого станет возможна повторная аутентификация. Диапазон значений: от 1 до 65535.

По умолчанию

Значение по умолчанию – 60 секунд.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Коммутатор будет в режиме молчания (Quiet State) после неудачной попытки аутентификации, пока не истечет таймер.

Пример

В данном примере показано, как настроить значение таймера повторной аутентификации для интерфейса Ethernet 1/0/1. Указанное значение – 20.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication timer restart 20
Switch(config-if)#
```

46.6 authentication username

Данная команда используется для создания пользователя в локальной базе данных аутентификации. Чтобы удалить пользователя из локальной базе данных аутентификации, воспользуйтесь формой **no** этой команды.

authentication username *NAME* **password** *PASSWORD* **[vlan** *VLAN-ID***]**
no authentication username *NAME* **[vlan]**

Параметры

NAME	Укажите имя пользователя. Максимальное количество символов – 32.
password *PASSWORD*	Укажите, чтобы задать пароль для MAC-аутентификации в обычном текстовом виде. Длина строки не может превышать 32 символа.
vlan *VLAN-ID*	Укажите, чтобы назначить VLAN.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить локальную базу данных для аутентификации пользователей.

Пример

В данном примере показано, как создать локальную учетную запись с именем пользователя user1 и паролем pass1.

```
Switch#configure terminal
Switch(config)#authentication username user1 password pass1
Switch(config)#
```

46.7 clear authentication sessions

Данная команда используется для удаления сессий аутентификации.

clear authentication sessions { dot1x | all | interface *INTERFACE-ID* **[dot1x] | mac-address** *MAC-ADDRESS***}**

Параметры

dot1x	Укажите для удаления всех сессий dot1x.
all	Укажите для удаления всех сессий.

interface *INTERFACE-ID*	Укажите для удаления сессий порта.
mac-address *MAC-ADDRESS*	Укажите для удаления всех сессий определенного пользователя.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Команда используется для удаления сессий аутентификации.

Пример

В данном примере показано, как удалить сессии аутентификации на интерфейсе Ethernet 1/0/1.

```
Switch#clear authentication sessions interface eth1/0/1
Switch#
```

46.8 authentication max users

Данная команда используется для настройки максимального количества аутентифицированных пользователей для всей системы или для порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

authentication max users *NUMBER*

no authentication max users

Параметры

NUMBER	Укажите, чтобы задать максимальное количество аутентифицированных пользователей. Доступен диапазон значений от 1 до 1000.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.
Interface Configuration Mode.

Использование команды

Команда применима в режиме Global Configuration Mode и Interface Configuration Mode.

Если команда настроена в режиме Global Configuration Mode, задается ограничение максимального количества пользователей на всю систему.

Если команда настроена в режиме Interface Configuration Mode, задается ограничение максимального количества пользователей на интерфейс.

Максимальное число пользователей включает пользователей 802.1X.

Также команда имеет следующие ограничения:

Если новое число максимального количества пользователей меньше, чем текущее количество пользователей, команда будет отклонена, и появится сообщение об ошибке.

Пример

В данном примере показано, как назначить максимальное количество аутентифицированных пользователей для системы.

```
Switch#configure terminal
Switch(config)#authentication max users 256
Switch(config)#
```

46.9 authorization disable

Данная команда используется для отключения приема авторизованной конфигурации. Чтобы включить принятие авторизованной конфигурации, воспользуйтесь формой **no** этой команды.

authorization disable
no authorization disable

Параметры

Нет.

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Команда используется для включения или отключения принятия авторизованной конфигурации. Если авторизация включена для аутентификации, авторизованные атрибуты (например, VLAN), назначенные RADIUS-сервером, будут приняты, если включено состояние авторизации.

Пример

В данном примере показано, как отключить состояние авторизации.

```
Switch#configure terminal
Switch(config)#no authorization disable
Switch(config)#
```

46.10 show authentication sessions

Данная команда используется для просмотра информации об аутентификации.

show authentication sessions [dot1x | interface *INTERFACE-ID* **[, | -] [dot1x] | mac-address** *MAC-ADDRESS***]**

Параметры

dot1x	(Опционально.) Укажите для отображения всех сессий dot1x.
interface *INTERFACE-ID*	(Опционально.) Укажите порт для отображения.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
mac-address *MAC-ADDRESS*	(Опционально.) Укажите для отображения определенного пользователя.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте команду без параметров, чтобы включить отображение сессий со всех портов.

Пример

В данном примере показано, как включить отображение сессий на интерфейсе Ethernet 1/0/1.

```
Switch#show authentication sessions interface eth1/0/1

Interface: eth1/0/1
MAC Address: 00-10-94-00-00-01
Authentication VLAN: 1
Authentication State: Success
Authentication Username: v4
Aging Time: 3600 sec
Method   State
  802.1X  : Success, Selected
  802.1X Authenticator State: AUTHENTICATED
  802.1X Backend State: IDLE

Total Authenticating Hosts: 0
Total Authenticated Hosts: 1
Total Blocked Hosts: 0

Switch#
```

Отображаемые параметры

Interface	Принимающий интерфейс узла аутентификации.
MAC Address	MAC-адрес узла аутентификации.
Authentication VLAN	Исходная VLAN начала аутентификации узла.
Authentication State	Состояние аутентификации узла. **Start** – принимается узел, но не было начала аутентификации **Initialization** – источник аутентификации готов, но новая аутентификация не начинается **Authenticating** – узел проходит аутентификацию **Failure** – ошибка аутентификации **Success** – узел прошел аутентификацию
Authentication Username	Имя пользователя узла.
Assigned VLAN	Назначенный VLAN ID, разрешенный после прохождения узлом аутентификации.
Aging Time/Block Time	**Aging Time** – время устаревания. Период времени, в течение которого узел аутентификации будет поддерживаться в аутентифицированном состоянии. По истечении данного времени узел вернется в неаутентифицированное состояние. **Blocked Time** – если узел не смог пройти аутентификацию, следующая попытка не начнется, пока не истечет время блокировки, если только пользователь не очистит состояние ввода entry state вручную.
Method	Метод аутентификации, например, 802.1X.
State	Состояние метода аутентификации. **Authenticating** – узел проходит аутентификацию с помощью данного метода **Success** – узел прошел аутентификацию с помощью данного метода аутентификации **Selected** – результат аутентификации данного метода, берется и анализируется системой для узла. **Failure** – узел не прошел аутентификацию с помощью данного метода **No Information** – информация об аутентификации недоступна.
802.1X Authenticator State	Состояние аутентификатора PAE 802.1X: возможны следующие значения: **INITIALIZE** – аутентификатор в процессе инициализации и ожидает запросов на аутентификацию. **DISCONNECTED** – инициализация завершена, но ни одно

	запрашивающее устройство не подключено к порту. **CONNECTING** – коммутатор обнаружил, что запрашивающее устройство подключается к порту. PAE произведет попытку установить подключение с запрашивающим устройством. **AUTHENTICATING** – запрашивающее устройство проходит аутентификацию. **AUTHENTICATED** – аутентификатор успешно аутентифицировал запрашивающее устройство. **ABORTING** – процедура аутентификации преждевременно отменена из-за запроса на повторную авторизацию, кадра EAPOL-Start, EAPOL-Logoff или тайм-айта аутентификации. **HELD** – коммутатор игнорирует или отбрасывает все EAPOL-пакеты для защиты от атак. В данное состояние можно перейти из состояния AUTHENTICATING после ошибки аутентификации. **FORCE_AUTH** – запрашивающее устройство всегда авторизовано **FORCE_UNAUTH** – запрашивающее устройство всегда не авторизовано.
802.1X Backend State	Состояние Backend PAE 802.1X. Возможны следующие значения: **REQUEST** – коммутатор получил пакет EAP-запроса от сервера аутентификации, и отправил пакет запрашивающему устройству в качестве EAPOL-инкапсулированного кадра. **RESPONSE** – коммутатор получил EAPOL-инкапсулированный пакет EAP-ответа от запрашивающего устройства и отправил EAP-пакет серверу аутентификации. **SUCCESS** – сервер аутентификации подтвердил, что запрашивающее устройство является допустимым клиентом. Backend уведомит аутентификатор PAE и запрашивающее устройство. **FAIL** – сервер аутентификации подтвердил, что запрашивающее устройство является недопустимым клиентом. Backend уведомит конечный автомат аутентификатор PAE и запрашивающее устройство. **TIMEOUT** – на сервере аутентификации или запрашивающем устройстве есть тайм-аут. **IDLE** – коммутатор ожидает начала новой сессии аутентификации. **INITIALIZE** – аутентификатор производит инициализацию.

47. Команды Network Protocol Port Protection

47.1 network-protocol-port protect

Данная команда используется, чтобы включить функцию защиты порта сетевого протокола. Для отключения функции воспользуйтесь формой **no** этой команды.

network-protocol-port protect {tcp | udp}
no network-protocol-port protect {tcp | udp}

Параметры

tcp	Укажите для защиты TCP-порта.
udp	Укажите для защиты UDP-порта.

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Команда применяется, чтобы включить или отключить функцию защиты порта сетевого протокола. Если порт защищен, коммутатор не будет отправлять ответные пакеты на закрытый TCP-порт или UDP-порт.

Пример

В данном примере показано, как включить защиту TCP-порта.

```
Switch#configure terminal
Switch(config)#network-protocol-port protect tcp
Switch(config)#
```

47.2 show network-protocol-port protect

Данная команда используется для отображения информации о защите порта сетевого протокола.

show network-protocol-port protect

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Команда применяется для отображения информации о защите порта сетевого протокола.

Пример

В данном примере показано, как отобразить информацию о защите порта сетевого протокола.

```
Switch#show network-protocol-port protect

    TCP Port protect state: Enabled
    UDP Port protect state: Enabled

Switch#
```

48. Команды Packet Debug

48.1 debug clear cpu counter

Данная команда используется для обнуления счетчиков пакетов, включая входящий и исходящий трафик порта ЦПУ.

debug clear cpu counter

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду для обнуления счетчиков пакетов, включая входящий и исходящий трафик порта ЦПУ, и повторного отсчета.

Пример

В данном примере показано, как обнулить счетчики пакетов ЦПУ.

```
Switch#debug clear cpu counter

Success

Switch#
```

48.2 debug dump packet_in_buffer

Данная команда используется для проверки полученных пакетов в буфере.

debug dump packet_in_buffer [len *LENGTH***] [count** *COUNT***] [channel** *CHANNEL***]**

Параметры

len *LENGTH*	(Опционально.) Укажите длину буфера печати для каждого пакета в байтах. Диапазон значений: от 0 до 2048.
count *COUNT*	(Опционально.) Укажите счетчик пакетов для каждого канала. Диапазон значений: от 1 до 200.
channel *CHANNEL*	(Опционально.) Укажите канал, который необходимо отобразить. Диапазон значений: от 1 до 4.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Команда используется для проверки полученных пакетов в буфере. Система поддерживает буферизацию до 200 пакетов на канал. Всего доступно 3 канала. Система будет записывать новые входящие пакеты в нижнюю позицию канала. При перегруженности системы полученные пакеты будут буферизироваться в верхнюю позицию. Пакеты в верхней позиции можно использовать для проверки причин перегруженности ЦПУ.

Пример

В данном примере показано, как отобразить пакеты канала 2.

```
Switch#debug dump packet_in_buffer channel 2

#=============================================================================
#ada69580-----------------------------------------------------------------
2019-01-01 00:02:41.506807 00 cnt 2, len 64,flags=4 port:1:1,DMA channel:2(FREE)
#>IP         ,EthRxNo    :  690,time:00000001(us,diff 1)
#>FreeMem    ,pkt_dbg.c  : 1331,time:00000102(us,diff 101)
0000: 00 57 a7 ad 10 01 f0 7d  68 12 10 01 81 00 80 01    .W.....}h.......
0010: 08 00 45 00 00 28 71 53  40 00 7f 06 c1 59 0a 5a    ..E..(qS@....Y.Z
0020: 5a 15 0a 5a 5a 5a c1 56  00 50 b6 60 8a 1f 01 e0    Z..ZZZ.V.P.`....
0030: a0 7d 50 10 3f 4a 02 e3  00 00                      .}P.?J....
#ada79780-----------------------------------------------------------------
2019-01-01 00:02:41.669789 01 cnt 2, len 64,flags=4 port:1:1,DMA channel:2(FREE)
#>IP         ,EthRxNo    :  756,time:00000002(us,diff 2)
#>FreeMem    ,pkt_dbg.c  : 1331,time:00000397(us,diff 395)
0000: 80 95 a6 ad 10 01 f0 7d  68 12 10 01 81 00 80 01    .......}h.......
0010: 08 00 45 00 00 28 71 95  40 00 7f 06 c1 17 0a 5a    ..E..(q.@......Z
0020: 5a 15 0a 5a 5a 5a c1 56  00 50 b6 60 8a 1f 01 e0    Z..ZZZ.V.P.`....
0030: e6 31 50 10 40 29 bc 4f  00 00                      .1P.@).O..
#=============================================================================
#Allocate packet memory 0, print 2
#Use '%Y-%m-%d %H:%M:%S.' as timestamp format string to import to wireshark

Switch#
```

48.3 debug show cpu counter

Данная команда используется для отображения счетчиков пакетов, включая входящий и исходящий трафик порта ЦПУ.

debug show cpu counter

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Команда используется для отображения счетчиков пакетов, включая входящий и исходящий трафик порта ЦПУ.

Пример

В данном примере показано, как отобразить счетчики пакетов порта ЦПУ.

```
Switch#debug show cpu counter

PacketType    TotalCounter     Pkt/Sec  PacketType    TotalCounter     Pkt/Sec
----------- ------RX-TX------ --RX-TX-- ----------- ------RX-TX------ --RX-TX--
UNKNOWN           0-0            0-0    1X_BPDU           0-0            0-0
STP_BPDU          0-0            0-0    GVRP_BPDU         0-0            0-0
IP              485-341          0-0    LACP_BPDU         0-0            0-0
BPDU              0-0            0-0    ARP            1296-3            0-0
IPv6              0-0            0-0    CTP               0-0            0-0
LLDP              0-0            0-0    DDPv4             0-0            0-0
DDPv6             0-0            0-0    DDP_L2            0-0            0-0
Stacking          0-0            0-0    Total          1781-344          0-0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

Отображаемые параметры

PacketType	Тип полученных пакетов каждого протокола.
TotalCounter	Все полученные и отправленные пакеты порта ЦПУ.

Pkt/Sec	Скорость входящего и исходящего трафика в пакетах в секунду.

49. Команды Port Security

49.1 clear port security

Данная команда используется для удаления динамически изученных безопасных MAC-адресов.

clear port-security {all | {address *MAC-ADDR* **| interface** *INTERFACE-ID* **[, | -]} [vlan** *VLAN-ID***]}**

Параметры

all	Укажите, чтобы удалить все динамически изученные безопасные MAC-адреса.
address *MAC-ADDR*	Укажите, чтобы удалить указанные динамически изученные безопасные записи на основе введенного MAC-адреса.
interface *INTERFACE-ID*	Укажите, чтобы удалить все динамически изученные безопасные записи на указанном интерфейсе.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
vlan *VLAN-ID*	Укажите, чтобы удалить динамически изученные записи, информация о которых была получена через указанную VLAN.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы удалить автоматически изученные безопасные MAC-адреса, как динамические, так и постоянные.

Пример

В данном примере показано, как удалить определенный безопасный адрес из таблицы MAC-адресов.

```
Switch# clear port-security address 0080.0070.0007
Switch#
```

49.2 show port-security

Данная команда используется для просмотра текущих настроек Port Security.

show port-security [interface *INTERFACE-ID* **[, | -]] [address]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите ID интерфейса для отображения.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
address	(Опционально.) Укажите для отображения безопасных MAC-адресов, включая настроенные и изученные адреса.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Команда применяется для отображения текущих настроек Port Security.

Пример

В данном примере показано, как отобразить настройки Port Security на портах 1-3.

```
Switch#show port-security interface eth1/0/1-3

 D:Delete-on-Timeout    P:Permanent
 Interface    Max  Curr   Violation    Violation   Security  Admin   Current
 No.          No.   No.     Act.       Count          Mode  State   State
 ------------ ----- ----- -------- ------------------- -- -------- ------------
 eth1/0/1     5     2     Restrict 0                   D  Enabled  Forwarding
 eth1/0/2     10    10    Shutdown 0                   D  Enabled  Err-disabled
 eth1/0/3     10    0     Shutdown 0                   P  Disabled -

Switch#
```

49.3 snmp-server enable traps port-security

Данная команда используется для включения отправки SNMP-уведомлений при обнаружении функционалом Port Security недопустимых адресов. Чтобы отключить отправку SNMP-уведомлений, воспользуйтесь формой **no** этой команды.

snmp-server enable traps port-security [trap-rate *TRAP-RATE***]**

no snmp-server enable traps port-security [trap-rate]

Параметры

trap-rate *TRAP-RATE*	(Опционально.) Укажите количество trap-сообщений в секунду. Диапазон значений: от 0 до 1000. Значение по умолчанию ("0") означает, что SNMP trap будет генерироваться для каждого нарушения безопасности.

По умолчанию

По умолчанию функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Команда применяется для включения или отключения отправки SNMP-уведомлений при обнаружении функционалом Port Security недопустимых адресов, а также для настройки количества trap-сообщений в секунду.

Пример

В данном примере показано, как включить отправку SNMP-уведомлений при обнаружении функционалом Port Security недопустимых адресов и установить количество trap-сообщений в секунду, равное 3.

```
Switch# configure terminal
Switch(config)#snmp-server enable traps port-security trap-rate 3
Switch(config)#
```

49.4 switchport port-security

Данная команда используется для настройки параметров Port Security, чтобы ограничить количество пользователей, которым разрешен доступ к порту. Чтобы отключить Port Security или удалить безопасный MAC-адрес, воспользуйтесь формой **no** этой команды.

switchport port-security [maximum *VALUE* **| violation {protect | restrict | shutdown} | mode {permanent | delete-on-timeout} | mac-address [permanent]** *MAC-ADDRESS* **[vlan** *VLAN-ID***]]**

no switchport port-security [maximum | violation | mode | mac-address [permanent] *MAC-ADDRESS* **[vlan** *VLAN-ID***]]**

Параметры

maximum *VALUE*	(Опционально.) Укажите максимальное число разрешенных безопасных MAC-адресов. Если не указано, значение по умолчанию – 32. Диапазон значений: от 0 до 64.
protect	(Опционально.) Укажите, если необходимо отбрасывать все пакеты с незащищенных узлов на уровне port-security без возрастания счетчика нарушения безопасности (security-violation).

restrict	(Опционально.) Укажите, если необходимо отбрасывать все пакеты с незащищенных узлов на уровне port-security, с возрастанием счетчика нарушения безопасности (security-violation) и записью в системный журнал (system log).
shutdown	(Опционально.) Укажите для отключения порта, если произошло нарушение безопасности и для записи в системный журнал.
permanent	(Опционально.) В данном режиме все изученные MAC-адреса не будут удалены, пока пользователь не удалит их вручную.
delete-on-timeout	(Опционально.) В данном режиме все изученные MAC-адреса будут удалены, когда запись устареет, или если пользователь удалит записи вручную.
mac-address *MAC-ADDRESS*	(Опционально.) Укажите, чтобы добавить безопасный MAC-адрес для получения доступа к порту.
permanent	(Опционально.) Укажите, чтобы задать безопасный постоянно настроенный MAC-адрес порта. Данная запись является такой же, как изученная в режиме Permanent Mode.
vlan *VLAN-ID*	(Опционально.) Укажите VLAN. Если VLAN не указана, MAC-адрес будет изучен в соответствии с PVID.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

При включении функции Port Security с режимом **delete-on-timeout**, порт будет автоматически изучать безопасные записи и хранить их, пока не истечет их тайм-аут. Время хранения этих записей зависит от настроек, заданных командой **switchport port-security aging**. Если режим порта задан как постоянный (permanent), он будет автоматически изучать безопасные записи с неистекающим тайм-аутом. Автоматически изученные безопасные записи будут храниться в текущем файле конфигурации (running configuration).

При изменении режима Port Security счетчик нарушений будет сброшен, автоматически изученные постоянные записи будут преобразованы в соответствующие динамические записи. При отключении Port Security автоматически изученные безопасные записи будут удалены, включая динамические и постоянные, счетчик нарушений будет сброшен. При изменении настройки VLAN автоматически изученные динамические безопасные записи будут удалены.

Постоянные безопасные записи будут храниться в текущем файле конфигурации и могут быть сохранены в NVRAM при помощи команды **copy**. Настроенные пользователем безопасные MAC-адреса будут подсчитываться в максимальном количестве MAC-адресов на порт.

Если на порту включена постоянная (permanent) безопасная запись Port Security, MAC-адрес нельзя перенести на другой порт.

При увеличении максимального числа разрешенных адресов изученные адреса останутся неизменными. Если максимальное число будет изменено на меньшее, чем существующее число изученных записей, команда будет отклонена.

У функции Port Security есть следующие ограничения:

Функция Port Security не может работать одновременно с 802.1X и IMPB, которые предоставляют более широкие возможности управления безопасностью.

Если порт указан в качестве порта назначения для функции зеркалирования, функция Port Security не может быть включена.

Если порт указан в качестве порта агрегирования каналов, функция Port Security не может быть включена.

При превышении максимального количества безопасных пользователей, может быть предпринято одно из следующих действий:

- **Protect** – когда число безопасных MAC-адресов порта достигает максимального значения пользователей, разрешенного на порту, пакеты с неизвестным адресом источника будут отбрасываться до тех пор, пока какая-нибудь безопасная запись не будет удалена.
- **Restrict** – при нарушении безопасности происходит ограничение данных, а также возрастает счетчик нарушений безопасности.
- **Shutdown** – при нарушении безопасности интерфейс отключается.

Пример

В данном примере показано, как настроить Port Security с режимом permanent с 5 безопасными MAC-адресами, разрешенными на порту.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security mode permanent
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)#
```

В примере ниже показано, как вручную добавить безопасный MAC-адрес 00-00-12-34-56-78 с VID 5 на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security mac-address 00-00-12-34-56-78 vlan 5
Switch(config-if)#
```

В следующем примере показано, как настроить отбрасывание всех пакетов от небезопасных узлов на уровне Port Security с увеличением счетчика нарушений при обнаружении нарушений безопасности.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)#
```

49.5 switchport port-security aging

Данная команда используется для указания времени устаревания (Aging Time) для динамически изученных безопасных адресов на интерфейсе. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

switchport port-security aging {time *MINUTES* **| type {absolute | inactivity}}**
no switchport port-security aging {time | type}

Параметры

time *MINUTES*	Укажите время устаревания (Aging Time) для динамически изученных безопасных адресов на порту в минутах. Диапазон значений: от 0 до 1440.
type	Укажите тип устаревания.
absolute	Укажите, чтобы задать тип absolute. Все безопасные адреса на данном порту устаревают строго после указанного времени и удаляются из списка безопасных адресов. Это тип по умолчанию.
inactivity	Укажите, чтобы задать тип inactivity. Все безопасные адреса на данном порту устаревают, только если нет трафика с безопасного адреса источника в течение указанного времени.

По умолчанию

По умолчанию функция отключена.

Время хранения по умолчанию – 0 минут.

Тип хранения по умолчанию – **absolute**.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Команда применяется для отключения процесса устаревания записей, а также для того чтобы указать время устаревания (Aging Time) динамически изученных безопасных записей. Для того чтобы задать тип **inactivity**, должна быть включена функция устаревания таблицы FDB.

Пример

В данном примере показано, как настроить время устаревания (Aging Time) динамически изученных безопасных MAC-адресов на порту 1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security aging time 1
Switch(config-if)#
```

49.6 port-security limit

Данная команда используется для указания максимального количества безопасных MAC-адресов в системе. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

port-security limit global *VALUE*
no port-security limit global

Параметры

VALUE	Укажите максимальное число записей Port Security, которое может быть изучено в системе. Диапазон значений: от 1 до 1792. Если указанное значение меньше текущего числа изученных записей, команда будет отклонена.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы ограничить количество изученных безопасных MAC-адресов в системе.

Пример

В данном примере показано, как настроить максимальное число безопасных MAC-адресов для системы.

```
Switch#configure terminal
Switch(config)#port-security limit global 100
Switch(config)#
```

50. Команды энергосбережения

50.1 dim led

Данная команда используется для отключения индикаторов портов с целью энергосбережения. Чтобы не отключать индикаторы портов, воспользуйтесь формой **no** этой команды.

dim led
no dim led

Параметры

Нет.

По умолчанию

По умолчанию данная функция выключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда применяется для отключения или включения индикаторов портов. Если данная функция включена, все индикаторы, отображающие статус порта, будут отключены с целью энергосбережения.

Пример

В данном примере показано, как отключить индикаторы портов с целью энергосбережения.

```
Switch# configure terminal
Switch(config)# dim led
Switch(config)#
```

50.2 power-saving

Данная команда используется для включения отдельных функций энергосбережения. Чтобы отключить данные функции, воспользуйтесь формой **no** этой команды.

power-saving {link-detection | port-shutdown | dim-led | hibernation}
no power-saving {link-detection | port-shutdown | dim-led | hibernation}

Параметры

link-detection	Укажите, чтобы включать функцию энергосбережения в зависимости от статуса соединения.
port-shutdown	Укажите, чтобы выполнять отключение портов по расписанию.

dim-led	Укажите, чтобы выполнять отключение индикаторов портов по расписанию.
hibernation	Укажите, чтобы включать режим сна системы по расписанию.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте нижеперечисленные параметры в команде для включения/отключения отдельных функций энергосбережения:
link-detection: устройство будет отключать неактивные порты в целях энергосбережения.
dim-led: устройство будет отключать индикаторы портов в указанный диапазон времени.
port-shutdown: устройство будет отключать все порты в указанный диапазон времени.
hibernation: устройство будет включать режима сна в указанный диапазон времени.

Пример

В данном примере показано, как настроить функцию энергосбережения с отключением портов и режимом сна по расписанию.

```
Switch# configure terminal
Switch(config)# power-saving port-shutdown
Switch(config)# power-saving hibernation
Switch(config)#
```

50.3 power-saving eee

Данная команда используется для включения функции Energy-Efficient Ethernet (EEE) на определенных портах. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

power-saving eee
no power-saving eee

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Команда применяется для включения или отключения функции Energy-Efficient Ethernet (EEE) на определенных портах. Режим EEE позволяет уменьшить энергопотребление при низком трафике пакетов на порту. Если передаваемые данные отсутствуют, на физическом интерфейсе будет включен режим Low Power Idle (LPI). В режиме EEE потребление питания изменяется в соответствии с изменениями текущей пропускной способности.

Пример

В данном примере показано, как включить функцию Power-Saving EEE.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# power-saving eee
Switch(config-if)#
```

50.4 power-saving dim-led time-range

Данная команда используется, чтобы настроить профиль временного диапазона для расписания отключения индикаторов. Для удаления профиля указанного диапазона времени воспользуйтесь формой **no** этой команды.

power-saving dim-led time-range *PROFILE-NAME*
no power-saving dim-led time-range *PROFILE-NAME*

Параметры

PROFILE-NAME	Укажите имя профиля временного диапазона, который необходимо настроить. Максимальное количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы добавить/удалить профиль временного диапазона для расписания отключения индикаторов. Если расписание настроено, индикаторы портов будут отключаться в соответствии с ним.

Пример

В данном примере показано, как добавить профиль временного диапазона для расписания отключения индикаторов.

```
Switch# configure terminal
Switch(config)# power-saving dim-led time-range off-duty
Switch(config)#
```

50.5 power-saving hibernation time-range

Данная команда используется для настройки профиля временного диапазона для расписания режима сна системы (hibernation). Используйте форму **no**, чтобы удалить профиль указанного диапазона времени.

power-saving hibernation time-range *PROFILE-NAME*
no power-saving hibernation time-range *PROFILE-NAME*

Параметры

PROFILE-NAME	Укажите имя профиля временного диапазона, который необходимо настроить. Максимальное количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы добавить/удалить профиль временного диапазона для расписания режима сна системы (hibernation). Когда система входит в режим сна, коммутатор начинает работать в состоянии низкого энергопотребления (режим ожидания). Отключаются все порты и индикаторы, сетевые функции не действуют. Будет работать только консольное соединение через порт RS232. Коммутатор, являющийся питающим устройством Power Sourcing Equipment (PSE), не будет обеспечивать порты электропитанием.

Пример

В данном примере показано, как добавить профиль временного диапазона для расписания режима сна системы.

```
Switch# configure terminal
Switch(config)# power-saving hibernation time-range off-duty
Switch(config)#
```

50.6 power-saving shutdown time-range

Данная команда используется, чтобы настроить профиль временного диапазона для расписания отключения порта. Для удаления профиля указанного диапазона времени воспользуйтесь формой **no** этой команды.

power-saving shutdown time-range *PROFILE-NAME*
no power-saving shutdown time-range *PROFILE-NAME*

Параметры

PROFILE-NAME	Укажите имя профиля временного диапазона, который необходимо настроить. Максимальное количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Используйте данную команду, чтобы добавить/удалить профиль временного диапазона для расписания отключения порта. Указанный порт будет отключаться в соответствии с настроенным расписанием.

Пример

В данном примере показано, как добавить профиль временного диапазона для расписания отключения порта.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# power-saving shutdown time-range off-duty
Switch(config-if)#
```

50.7 show power-saving

Данная команда используется для отображения информации о настройках энергосбережения.

show power-saving [link-detection] [dim-led] [port-shutdown [hibernation] [eee]

Параметры

link-detection	(Опционально.) Укажите, чтобы отобразить настройки энергосбережения в зависимости от статуса соединения.
dim-led	(Опционально.) Укажите, чтобы отобразить состояние индикаторов.
port-shutdown	(Опционально.) Укажите, чтобы отобразить настройки энергосбережения, связанные с отключением порта.
hibernation	(Опционально.) Укажите, чтобы отобразить настройки энергосбережения для режима сна.
eee	(Опционально.) Укажите, чтобы отобразить состояние функции EEE.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если параметры не указаны, будет отображена информация обо всех настройках энергосбережения.

Пример

В данном примере показано, как отобразить информацию обо всех настройках энергосбережения.

```
Switch#show power-saving
Function Version: 3.00

Link Detection Power Saving
  State: Disabled

Scheduled Hibernation Power Saving
  State: Disabled

Administrative Dim-LED
  State: Disabled

Scheduled Dim-LED Power Saving
  State: Disabled

Scheduled Port-shutdown Power Saving
  State: Disabled

EEE_Enabled Ports

Switch#
```

51. Команды Protocol Independent

51.1 ip route

Данная команда используется для создания записи статического маршрута. Чтобы удалить запись статического маршрута, воспользуйтесь формой **no** этой команды.

ip route *NETWORK-PREFIX NETWORK-MASK IP-ADDRESS* **[primary | backup]**
no ip route *NETWORK-PREFIX NETWORK-MASK IP-ADDRESS*

Параметры

NETWORK-PREFIX	Укажите сетевой адрес.
NETWORK-MASK	Укажите сетевую маску.
IP-ADDRESS	Укажите IP-адрес следующего узла, который будет использоваться для достижения сети назначения.
primary	(Опционально.) Указывает, что маршрут будет использоваться в качестве основного.
backup	(Опционально.) Указывает, что маршрут будет использоваться в качестве резервного.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы создать IP статического маршрута. Поддерживаются резервные маршруты. Это означает, что можно создать два маршрута с одним адресом сети назначения, но с разными следующими узлами. Если параметры **primary** или **backup** не указаны, статический маршрут будет автоматически определен как основной или резервный. Основной маршрут считается предпочтительным. Если он становится недоступным, будет использоваться резервный маршрут.

Пример

В данном примере показано, как добавить запись статического маршрута. Сетевой адрес – 20.0.0.0/8. Следующий узел – 10.1.1.254.

```
Switch# configure terminal
Switch(config)# ip route 20.0.0.0 255.0.0.0 10.1.1.254
Switch(config)#
```

51.2 ipv6 route

Данная команда используется для создания записи статического маршрута IPv6. Для удаления записи статического маршрута IPv6 воспользуйтесь формой **no** этой команды.

ipv6 route {default | *NETWORK-PREFIX/PREFIX-LENGTH***} [***INTERFACE-ID***]** *NEXT-HOP-ADDRESS* **[primary | backup]**

no ipv6 route {default | *NETWORK-PREFIX/PREFIX-LENGTH***} [***INTERFACE-ID***]** *NEXT-HOP-ADDRESS*

Параметры

default	Укажите, чтобы добавить или удалить маршрут по умолчанию.
NETWORK-PREFIX/PREFIX-LENGTH	Укажите сетевой префикс и длину префикса статического маршрута.
INTERFACE-ID	(Опционально.) Укажите интерфейс передачи для маршрутизации пакетов.
NEXT-HOP-ADDRESS	Укажите IPv6-адрес следующего узла (next hop), который будет использоваться для достижения сети назначения. Если адрес является адресом link-local, необходимо также указать ID интерфейса.
primary	(Опционально.) Указывает, что маршрут будет использоваться в качестве основного статического маршрута.
backup	(Опционально.) Указывает, что маршрут будет использоваться в качестве резервного статического маршрута.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Поддерживаются резервные маршруты. Это означает, что можно создать два маршрута с одним адресом сети назначения, но с разными следующими узлами. Если параметры **primary** или **backup** не указаны, статический маршрут будет автоматически определен как основной или резервный. Основной маршрут считается предпочтительным и всегда используется для продвижения, если находится в активном режиме. Если он становится недоступным, будет использоваться резервный маршрут.

Пример

В данном примере показано, как создать статический маршрут для сети, в которой находится прокси-сервер.

```
Switch# configure terminal
Switch(config)# ipv6 route 2001:0101::/32 vlan1 fe80::0000:00ff:1111:2233
Switch(config)#
```

51.3 show ip route

Данная команда используется для отображения записей таблицы маршрутизации.

show ip route [*IP-ADDRESS* **[***MASK***] | connected | static | hardware]**

Параметры

IP-ADDRESS	(Опционально.) Укажите сетевой адрес, информацию о маршрутизации которого необходимо отобразить.
MASK	(Опционально.) Укажите маску подсети для указанной сети.
connected	(Опционально.) Укажите, чтобы отобразить подключенный маршрут.
static	(Опционально.) Укажите, чтобы отобразить статический маршрут.
hardware	(Опционально.) Укажите для отображения маршрутов, записанных в чипсет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить самые приоритетные маршруты, которые являются текущей записью маршрута.

Пример

В данном примере показано, как отобразить таблицу маршрутизации.

```
Switch#show ip route
Code: C - connected, S - static
      * - candidate default


Gateway of last resort is 10.1.1.254 to network 0.0.0.0

S*   0.0.0.0/0 [1/1] via 10.1.1.254, vlan1
C    10.0.0.0/8 is directly connected, vlan1

Total Entries: 2


Switch#
```

51.4 show ip route summary

Данная команда используется для отображения краткой информации о текущих записях маршрутизации.

show ip route summary

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения краткой информации о текущих записях маршрутизации.

Пример

В данном примере показано, как отобразить краткую информацию о текущих записях маршрутизации.

```
Switch# show ip route summary

Route Source    Networks
Connected       1
Static          0
Total           1

Switch#
```

51.5 show ipv6 route

Данная команда используется для отображения записей таблицы маршрутизации.

show ipv6 route [[*IPV6-ADDRESS* **|** *NETWORK-PREFIX/PREFIX-LENGTH* **| interface** *INTERFACE-ID* **|** *PROTOCOL***] [database] | hardware]**

Параметры

IPV6-ADDRESS	(Опционально.) Укажите IPv6-адрес, чтобы найти самый длинный префикс соответствующего IPv6-маршрута.
NETWORK-PREFIX/PREFIX-LENGTH	(Опционально.) Укажите сетевой адрес, информацию о маршрутизации которого необходимо отобразить.
interface *INTERFACE-ID*	(Опционально.) Укажите интерфейс, который необходимо отобразить.
PROTOCOL	(Опционально.) Укажите протокол маршрутизации: **static** или **connected**.
database	(Опционально.) Укажите, чтобы отобразить все соответствующие записи в таблице маршрутизации, а не только приоритетный маршрут.
hardware	(Опционально.) Укажите для отображения маршрутов, записанных в чипсет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить записи таблицы маршрутизации.

Пример

В данном примере показано, как отобразить записи маршрутизации для IPv6.

```
Switch#show ipv6 route

IPv6 Routing Table
Code: C - connected, S - static
      SLAAC - Stateless address autoconfiguration

C     2000:410:1::/64 [0/1] is directly connected, vlan1
S     2001:0101::/64 [1/1] via fe80::0000:00ff:1111:2233, vlan1
S     2001:0102::/64 [1/1] via fe80::0000:00ff:1111:2233, vlan1

Total Entries: 3 entries, 3 routes
Switch#
```

51.6 show ipv6 route summary

Данная команда используется для отображения краткой информации о текущих записях таблицы маршрутизации IPv6.

show ipv6 route summary

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если система обеспечивает маршрутизацию IPv6-трафика, проверка таблицы маршрутизации помогает понять, как в данный момент перенаправляется трафик в сети.

Пример

В данном примере показано, как отобразить краткую информацию о текущих записях таблицы маршрутизации IPv6.

```
Switch#show ipv6 route summary

Route Source    Networks
Connected       2
Static          1
SLAAC           0
Total           3

Switch#
```

52. Команды Quality of Service (QoS)

52.1 class

Данная команда используется, чтобы указать имя карты класса (class map) для привязки к политике трафика и войти в режим Policy-map Configuration Mode. Чтобы удалить описание политики указанного класса, воспользуйтесь формой **no** этой команды.

class *NAME*
no class *NAME*
class class-default

Параметры

NAME	Укажите имя карты класса (class map) для привязки к политике трафика.

По умолчанию

Нет.

Режим ввода команды

Policy-map Configuration Mode.

Использование команды

После ввода данной команды будет выполнен вход в режим Policy-map Configuration Mode. Весь трафик, который не соответствует текущему настроенному классу, будет классифицирован как класс по умолчанию (class-default). Если указанного имени карты класса (class map) не существует, никакой трафик не классифицируется в класс.

Пример

В данном примере показано, как настроить карту политики (policy map), в которой определены политики для класса «class-dscp-red». Настроенная карта политики – policy1. Все пакеты, соответствующие DSCP-меткам 10, 12 или 14, будут маркированы в качестве DSCP 10.

```
Switch# configure terminal
Switch(config)# class-map class-dscp-red
Switch(config-cmap)# match ip dscp 10,12,14
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class class-dscp-red
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap-c)#
```

52.2 class-map

Данная команда используется для входа в режим Class-map Configuration Mode или для создания/изменения карты класса, в которой определены критерии соответствия пакетов. Чтобы удалить существующую карту класса на коммутаторе, воспользуйтесь формой **no** этой команды.

class-map [match-all | match-any] *NAME*
no class-map *NAME*

Параметры

match-all	(Опционально.) Укажите, чтобы критерии соответствия карты класса были оценены на основе логического AND. Если ключевое слово **match-all** или **match-any** не указано, по умолчанию будет использовано **match-any**.
match-any	(Опционально.) Укажите, чтобы критерии соответствия карты класса были оценены на основе логического OR. Если ключевое слово **match-all** или **match-any** не указано, по умолчанию будет использовано **match-any**.
NAME	Укажите имя карты класса. Максимальное количество символов – 32.

По умолчанию

По умолчанию используется только class-default.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы создать или изменить карту класса, в которой определены критерии соответствия пакетов, настраиваемые в режиме Class-map Configuration Mode.

Если для класса применено несколько команд соответствия, необходимо использовать ключевое слово **match-all** или **match-any**, чтобы указать, на основе чего (логического AND или логического OR) будут оцениваться критерии соответствия.

Пример

В данном примере показано, как настроить имя карты класса. Указанное имя – class_home_user. Условие соответствия для данной карты класса выполняется, если трафик, соответствующий списку управления доступом «acl_home_user» и протоколу IPv6, будет включен в заданную карту класса «class_home_user».

```
Switch#configure terminal
Switch(config)#class-map match-all class_home_user
Switch(config-cmap)#match access-group name acl_home_user
Switch(config-cmap)#match protocol ipv6
Switch(config-cmap)#
```

52.3 match

Данная команда используется, чтобы настроить критерии соответствия для карты класса. Для удаления критериев соответствия воспользуйтесь формой **no** этой команды.

match {access-group name *ACCESS-LIST-NAME* **| cos** *COS-LIST* **| [ip] dscp** *DSCP-LIST* **| [ip] precedence** *IP-PRECEDENCE-LIST* **| protocol** *PROTOCOL-NAME* **| vlan** *VLAN-ID-LIST***}**

no match {access-group name *ACCESS-LIST-NAME* **| cos** *COS-LIST* **| [ip] dscp** *DSCP-LIST* **| [ip] precedence** *IP-PRECEDENCE-LIST* **| protocol** *PROTOCOL-NAME* **| vlan** *VLAN-ID-LIST***}**

Параметры

access-group name *ACCESS-LIST-NAME*	Укажите список доступа в качестве критерия соответствия. Трафик, разрешенный указанным списком доступа, будет классифицирован.
cos *COS-LIST*	Укажите значение (-я) определенного IEEE 802.1Q в качестве критерия соответствия. Диапазон значений: от 0 до 7. Для перечисления нескольких значений CoS используется запятая, а для обозначения диапазона значений – дефис.
[ip] dscp *DSCP-LIST*	Укажите значения DSCP-метки в качестве критерия соответствия. Диапазон значений: от 0 до 63. Для перечисления нескольких значений DSCP используется запятая, а для обозначения диапазона значений – дефис. **ip** – (Опционально.) Укажите, чтобы настроить критерий соответствия только для пакетов IPv4. Если не указано, критерий соответствия настраивается для пакетов IPv4 и IPv6.
[ip] precedence *IP-PRECEDENCE-LIST*	Укажите значения приоритета IP в качестве критерия соответствия. Диапазон значений: от 0 до 7. Для перечисления нескольких значений приоритета используется запятая, а для обозначения диапазона значений – дефис. **ip** – (Опционально.) Укажите, чтобы настроить критерий соответствия только для пакетов IPv4. Если не указано, критерий соответствия настраивается для пакетов IPv4 и IPv6. Для пакетов IPv6 приоритетом являются три наиболее значимых бита класса трафика заголовка IPv6.
protocol *PROTOCOL-NAME*	Укажите имя протокола в качестве критерия соответствия.
vlan *VLAN-ID-LIST*	Укажите номер (-а) или диапазон номеров идентификации VLAN в качестве критерия соответствия. Диапазон значений: от 1 до 4094. Для перечисления нескольких значений VLAN используется запятая, а для обозначения диапазона значений – дефис.

По умолчанию

Нет.

Режим ввода команды

Class-map Configuration Mode.

Использование команды

Перед применением данной команды используйте команду **class-map**, чтобы указать имя класса, для которого будут настроены критерии соответствия. Политика обработки данных соответствующих пакетов настраивается в режиме Policy-map Class Configuration Mode.

В списке ниже представлены протоколы, доступные для данной команды:

- **arp** - IP Address Resolution Protocol (ARP)
- **bgp** - Border Gateway Protocol
- **dhcp** - Dynamic Host Configuration
- **dns** - Domain Name Server lookup
- **egp** - Exterior Gateway Protocol
- **ftp** - File Transfer Protocol
- **ip** - IP (version 4)
- **ipv6** - IP (version 6)
- **netbios** – NetBIOS
- **nfs** - Network File System
- **ntp** - Network Time Protocol
- **ospf** - Open Shortest Path First
- **pppoe** - Point-to-Point Protocol over Ethernet
- **rip** - Routing Information Protocol
- **rtsp** - Real-Time Streaming Protocol
- **ssh** - Secured shell
- **telnet** - Telnet
- **tftp** - Trivial File Transfer Protocol

Пример

В данном примере показано, как настроить карту класса и список доступа, который будет использован в качестве критерия соответствия для данного класса. Имя заданной карты класса – class-home-user. Имя указанного списка доступа – acl-home-user.

```
Switch#configure terminal
Switch(config)#class-map class-home-user
Switch(config-cmap)#match access-group name acl-home-user
Switch(config-cmap)#
```

В примере ниже показано, как настроить карту класса и значения CoS, которые будут использованы в качестве критериев соответствия для данного класса. Имя заданной карты класса – cos. Указанные значения CoS – 1, 2 и 3.

```
Switch#configure terminal
Switch(config)#class-map cos
Switch(config-cmap)#match cos 1,2,3
Switch(config-cmap)#
```

52.4 mls qos cos

Данная команда используется, чтобы настроить значение CoS по умолчанию для порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

mls qos cos {*COS-VALUE* **| override}**
no mls qos cos

Параметры

COS-VALUE	Укажите значение CoS по умолчанию, которое будет применено к входящим нетегированным пакетам, полученным на порту.
override	Укажите, чтобы отменить CoS пакетов. Для всех полученных на порту пакетов (тегированных и нетегированных) будет применен CoS по умолчанию.

По умолчанию

Значение CoS по умолчанию – 0.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Если параметр **override** не указан, для тегированных пакетов применяется CoS, назначенный пакету; для нетегированных пакетов будет применен CoS по умолчанию.

Если параметр **override** указан, для всех полученных на порту пакетов будет применен CoS по умолчанию. Используйте ключевое слово **override**, если все входящие пакеты на определенных портах заслуживают приоритет выше или ниже, чем пакеты, поступающие из других портов. При использовании данной команды, ранее настроенные доверенные DSCP и CoS будут перезаписаны, и все значения CoS входящих пакетов будут изменены на CoS по умолчанию, настроенный в команде **mls qos cos**. Если входящие пакеты тегированные, их значение CoS изменяется на входном порту.

Пример

В данном примере показано, как настроить значение CoS по умолчанию на интерфейсе Ethernet 1/0/1. Заданное значение – 3.

```
Switch#configure terminal
Switch(config)#interface  eth1/0/1
Switch(config-if)#mls qos cos 3
Switch(config-if)#
```

52.5 mls qos dscp-mutation

Данная команда используется для привязки карты изменения входящего DSCP (DSCP Mutation) к интерфейсу. Чтобы удалить привязку карты DSCP Mutation к интерфейсу, воспользуйтесь формой **no** этой команды.

mls qos dscp-mutation *DSCP-MUTATION-TABLE-NAME*
no mls qos dscp-mutation

Параметры

DSCP-MUTATION-TABLE-NAME	Укажите имя таблицы DSCP Mutation без пробелов. Максимальное количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Используйте данную команду, чтобы привязать таблицу DSCP Mutation к интерфейсу. Значение DSCP пакета, полученного на интерфейсе, будет изменено с помощью DSCP Mutation. Пакет с новым значением DSCP будет обработан QoS и отправлен из порта коммутатора.

Пример

В данном примере показано, как преобразовать значение DSCP и привязать карту изменений внутреннего DSCP (DSCP Mutation) к интерфейсу Ethernet 1/0/1. Ранее настроенное значение DSCP – 30. Новое значение – 8. Карта DSCP Mutation – mutemap1.

```
Switch#configure terminal
Switch(config)#mls qos map dscp-mutation mutemap1 30 to 8
Switch(config)#interface eth1/0/1
Switch(config-if)#mls qos dscp-mutation mutemap1
Switch(config-if)#
```

52.6 mls qos map dscp-cos

Данная команда используется для привязки DSCP-меток к CoS. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

mls qos map dscp-cos *DSCP-LIST* **to** *COS-VALUE*
no mls qos map dscp-cos *DSCP-LIST*

Параметры

dscp-cos *DSCP-LIST* **to** *COS-VALUE*	Укажите список DSCP-меток для привязки к значению CoS. Диапазон значений: от 0 до 63. Используйте дефис, чтобы отделить диапазон значений. Используйте запятую, чтобы разделить несколько значений. Пробелы и дефисы до и после символов недопустимы.
DSCP-LIST	Укажите диапазон DSCP-меток.

По умолчанию

Значение CoS:	0	1	2	3	4	5	6	7
Значение DSCP:	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда позволяет привязать DSCP-метку доверенного порта DSCP к значению внутреннего CoS. Данное значение CoS будет привязано к очереди CoS на основе CoS в карте очереди, настроенной в команде **priority-queue cos-map**.

Пример

В данном примере показано, как привязать DSCP к CoS на интерфейсе Ethernet 1/0/6. DSCP-метки 12, 16 и 18 привязаны к CoS 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/6
Switch(config-if)#mls qos map dscp-cos 12,16,18 to 1
Switch(config-if)#
```

52.7 mls qos map dscp-mutation

Данная команда используется для настройки карты DSCP Mutation. Чтобы удалить карту Mutation, воспользуйтесь формой **no** этой команды.

mls qos map dscp-mutation *MAP-NAME INPUT-DSCP-LIST* **to** *OUTPUT-DSCP*
no mls qos map dscp-mutation *MAP-NAME*

Параметры

MAP-NAME	Укажите имя карты DSCP Mutation. Максимальное количество символов – 32. Пробелы недопустимы.
INPUT-DSCP-LIST	Укажите список DSCP, значения которых необходимо «мутировать». Диапазон значений: от 0 до 63. Используйте дефис, чтобы отделить диапазон значений. Используйте запятую, чтобы разделить несколько значений. Пробелы и дефисы до и после символов недопустимы.
OUTPUT-DSCP	Укажите значение DSCP, которое будет применено после «мутации» Mutation. Диапазон значений: от 0 до 63.

По умолчанию

По умолчанию параметры *OUTPUT-DSCP* и *INPUT-DSCP* равны.

Режим ввода команды

Global Configuration Mode.

Использование команды

Значение внутреннего DSCP пакета, полученного на интерфейсе, будет изменено на основе карты DSCP Mutation перед другими QoS-операциями. DSCP Mutation способствует объединению доменов с разными назначениями DSCP.

При настройке карты DSCP Mutation обратите внимание на то, что для каждых новых значений DSCP, которые нужно изменить, и для каждых новых значений, которые будут применены после «мутации» Mutation, необходимо использовать команду несколько раз.

Привязка DSCP-CoS будет основываться на исходном DSCP пакета, а все последующие действия – на значении DSCP, которое будет применено после «мутации» Mutation.

Пример

В данном примере показано, как преобразовать DSCP 30 в DSCP 8 и DSCP 20 в DSCP 10. Имя карты Mutation – mutemap1.

```
Switch#configure terminal
Switch(config)#mls qos map dscp-mutation mutemap1 30 to 8
Switch(config)#mls qos map dscp-mutation mutemap1 20 to 10
Switch(config)#
```

52.8 mls qos scheduler

Данная команда используется для настройки механизма обслуживания очередей. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

mls qos scheduler {sp | rr | wrr | wdrr}
no mls qos scheduler

Параметры

sp	Укажите алгоритм Strict Priority, SP для всех очередей.
rr	Укажите алгоритм Round-Robin, RR для всех очередей.
wrr	Укажите алгоритм Weighted Round-Robin, WRR по числу кадров для всех очередей. Если настроенный вес (weight) очереди равен нулю, для данной очереди будет включен алгоритм Strict Priority, SP.
wdrr	Укажите алгоритм Weighted Deficit Round-Robin, WDRR по длине кадров (quantum) для очередей всех портов. Если настроенный вес (weight) очереди равен нулю, для данной очереди включен алгоритм Strict Priority, SP.

По умолчанию

Алгоритм механизма обслуживания очередей для очереди по умолчанию – WRR.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Укажите алгоритм обслуживания очередей (WRR, SP, RR или WDRR) для выходной очереди. Алгоритм обслуживания очередей для очереди по умолчанию – WRR. WDRR предназначен для набора накопившихся кредитов в очереди передачи в режиме Round-Robin. Изначально для каждой очереди установлен свой счетчик кредита (настроенное значение quantum). Каждый раз, когда пакет

отправляется из очереди CoS, размер пакета вычитается из соответствующего счетчика кредитов, и право на обслуживание переходит к очереди с более низким CoS. Если счетчик кредитов опускается ниже нуля, очередь не обслуживается до тех пор, пока ее кредиты не будут снова пополнены. Счетчики кредитов всех очередей CoS при достижении нуля пополняются за одни раз.

Обслуживание всех пакетов прекращается, когда их счетчики достигают нуля или становятся меньше нуля, а также после полного осуществления передачи последнего пакета. При выполнении данного условия к каждому счетчику в очереди CoS будет добавлено значение quantum кредитов. Значение quantum для каждой очереди может отличаться в зависимости от пользовательских настроек.

Для включения режима Strict Priority для очереди CoS необходимо, чтобы для всех других очередей CoS с более высоким приоритетом также был установлен режим Strict Priority.

WRR предназначен для передачи разрешенных пакетов в очереди передачи в режиме Round-Robin. Изначально вес каждой очереди установлен на основе настроенного веса. Каждый раз, когда пакет отправляется из очереди CoS с более высоким приоритетом, из соответствующего веса вычитается 1, и право на обслуживание переходит к пакету из очереди CoS с приоритетом ниже предыдущего. Если вес очереди CoS достигает нуля, очередь не обслуживается до тех пор, пока ее вес не будет возобновлен. Вес всех очередей CoS при достижении нуля возобновляется за один раз.

Пример

В данном примере показано, как настроить алгоритм Strict Priority, SP для очереди.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mls qos scheduler sp
Switch(config-if)#
```

52.9 mls qos trust

Данная команда используется, чтобы настроить доверенный статус (trust) на порту для поля CoS или DSCP поступающего пакета для последующих QoS-операций. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

mls qos trust {cos | dscp}
no mls qos trust

Параметры

cos	Укажите, чтобы назначить биты CoS поступающих пакетов доверенными для последующих QoS-операций.
dscp	Укажите, чтобы назначить биты ToS/DSCP (если доступны в поступающих пакетах) доверенными для последующих операций. Для не IP-пакетов: доверенной будет назначена информация 2 уровня CoS для классификации трафика.

По умолчанию

По умолчанию доверенным является CoS.

Режим ввода команды

Interface Configuration Mode.

Использование команды

После настройки статуса trust для DSCP на интерфейсе, для последующих QoS-операций DSCP приходящих пакетов будет доверенным. Сначала DSCP будет привязан к значению внутреннего CoS, которое в дальнейшем будет использовано для определения очереди CoS. Привязка DSCP к CoS настраивается с помощью команды **mls qos map dscp-cos**. Чтобы настроить CoS в карте очереди, используйте команду **priority-queue cos-map**. Если приходящий пакет не IP-пакет, доверенным будет CoS. В передаваемом пакете также будет CoS, полученный в результате привязки DSCP.

После настройки статуса trust для CoS на интерфейсе, CoS приходящих пакетов будет применен в качестве внутреннего CoS и использован для определения очереди CoS. Очередь CoS определяется на основе таблицы соответствия CoS и очереди.

Пакету, прибывшему на порт 802.1Q VLAN tunnel, будет добавлен внешний тег VLAN для передачи через VLAN tunnel. Если на порту настроен статус trust для CoS, тег внутреннего CoS будет являться CoS пакета и значением CoS во внешнем теге VLAN пакета. Если при вводе команды **mls qos cos** был указан параметр **override**, то внутренним CoS пакета и значением CoS во внешнем теге VLAN пакета будет CoS, настроенный в команде **mls qos cos**. Если на порту настроен статус trust для DSCP, то внутренним CoS пакета и значением CoS во внешнем теге VLAN пакета будет CoS, полученный в результате привязки DSCP.

Пример

В данном примере показано, как настроить режим trust для DSCP на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mls qos trust dscp
Switch(config-if)#
```

52.10 policy-map

Данная команда используется для входа в режим Policy-map Configuration Mode и создания/изменения карты политики, которая может быть привязана к одному или нескольким интерфейсам в качестве политики обслуживания. Чтобы удалить карту политики, воспользуйтесь формой **no** этой команды.

policy-map *NAME*
no policy-map *NAME*

Параметры

NAME	Укажите имя карты политики. Максимальное количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте команду **policy-map**, чтобы войти в режим Policy-map Configuration Mode и настроить/изменить политику для класса трафика. Одна карта политики может быть привязана к нескольким интерфейсам одновременно. Предыдущие привязки карты политики будут перезаписаны новыми.

Карты политики содержат классы трафика, которые включают в себя одну или более команд для соответствия пакетов и для организации пакетов в группы на основе типа протокола или приложения.

Пример

В данном примере показано, как создать карту политики под именем «policy» и настроить для нее две политики класса. Первый класс «class1» указывает политику для трафика, соответствующего списку управления доступом (ACL) «acl_rd». Второй класс является классом по умолчанию «class-default». В данный класс включены пакеты, которые не соответствуют настроенным классам.

```
Switch#configure terminal
Switch(config)#class-map class1
Switch(config-cmap)#match access-group name acl_rd
Switch(config-cmap)#exit
Switch(config)#policy-map policy
Switch(config-pmap)#class class1
Switch(config-pmap-c)#set ip dscp 46
Switch(config-pmap-c)#exit
Switch(config-pmap)#class class-default
Switch(config-pmap-c)#set ip dscp 0
Switch(config-pmap-c)#
```

52.11 priority-queue cos-map

Данная команда используется для привязки CoS к карте очереди. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

priority-queue cos-map *QUEUE-ID COS1* **[***COS2* **[***COS3* **[***COS4* **[***COS5* **[***COS6* **[***COS7* **[***COS8***]]]]]]]**

no priority-queue cos-map

Параметры

QUEUE-ID	Укажите ID очереди, к которой будет привязан CoS.
CoS 1	Укажите значение CoS для привязки. Диапазон значений: от 0 до 7.
COS2...COS8	(Опционально.) Укажите значение CoS для привязки. Диапазон значений: от 0 до 7.

По умолчанию

По умолчанию привязка приоритета CoS к очереди: 0 к 2, 1 к 0, 2 к 1, 3 к 3, 4 к 4, 5 к 5, 6 к 6, 7 к 7.

Режим ввода команды

Global Configuration Mode.

Использование команды

Полученному пакету присваивается внутренний CoS, который используется для выбора очереди передачи на основе привязки карты CoS к карте очереди. Чем выше значение CoS очереди, тем выше приоритет.

Пример

В данном примере показано, как привязать приоритет CoS 3, 5 и 6 к очереди 2.

```
Switch#configure terminal
Switch(config)#priority-queue cos-map 2 3 5 6
Switch(config)#
```

52.12 queue rate-limit

Данная команда позволяет указать/изменить полосу пропускания (bandwidth), предназначенную для очереди. Чтобы удалить полосу пропускания, предназначенную для очереди, воспользуйтесь формой **no** этой команды.

queue *QUEUE-ID* **rate-limit {***MIN-BANDWIDTH-KBPS* **| percent** *MIN-PERCENTAGE***} {***MAX-BANDWIDTH-KBPS* **| percent** *MAX-PERCENTAGE***}**

no queue *QUEUE-ID* **rate-limit**

Параметры

QUEUE-ID	Укажите ID очереди, для которой необходимо настроить минимальную разрешенную и максимальную полосу пропускания.
MIN-BANDWIDTH-KBPS	Укажите минимальную разрешенную полосу пропускания в Кбит/с для указанной очереди.
MAX-BANDWIDTH-KBPS	Укажите максимальную полосу пропускания в Кбит/с для указанной очереди.
MIN-PERCENTAGE	Укажите минимальную полосу пропускания в процентах. Диапазон значений: от 1 до 100.
MAX-PERCENTAGE	Укажите максимальную полосу пропускания в процентах. Диапазон значений: от 1 до 100.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить минимальную и максимальную полосу пропускания для определенной очереди. Если минимальная полоса пропускания настроена, пакет, передаваемый

из данной очереди, гарантирован. Если настроена максимальная полоса пропускания, пакеты, передаваемые из данной очереди, не могут превышать максимальную полосу пропускания, даже если полоса пропускания доступна.

Значение всей минимальной полосы пропускания должно быть меньше 75 процентов полосы пропускания интерфейса. Для очереди с наивысшим приоритетом настройка минимальной разрешенной полосы пропускания необязательна, так как трафик данной очереди обслуживается в первую очередь, если все очереди соответствуют заданной минимальной полосе пропускания.

Данная команда применима исключительно для настройки физического порта; для port-channel команда недоступна. На физических портах невозможна настройка минимальной разрешенной полосы пропускания одного CoS.

Пример

В данном примере показано, как настроить полосу пропускания очереди для интерфейса Ethernet 1/0/1. Для очереди 1 «queue 1» заданы минимальная разрешенная полоса пропускания 100 Кбит/с и максимальная полоса пропускания 2000 Кбит/с. Для очереди 2 «queue 2» указаны минимальная разрешенная полоса пропускания 10% и максимальная полоса пропускания 50%.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#queue 1 rate-limit 100 2000
Switch(config-if)#queue 2 rate-limit percent 10 percent 50
Switch(config-if)#
```

52.13 rate-limit {input | output}

Данная команда используется, чтобы настроить значения ограничения полосы пропускания для входящего и исходящего трафика на интерфейсе. Для отмены ограничения полосы пропускания воспользуйтесь формой **no** этой команды.

rate-limit {input | output} {*NUMBER-KBPS* **| percent** *PERCENTAGE***} [***BURST-SIZE***]**
no rate-limit {input | output}

Параметры

input	Укажите ограничение полосы пропускания для входящих пакетов.
output	Укажите ограничение полосы пропускания для исходящих пакетов.
NUMBER-KBPS	Укажите ограничение максимальной полосы пропускания в Кбит/с.
PERCENTAGE	Укажите для настройки ограничения в процентах. Диапазон значений: от 1 до 100.
BURST-SIZE	(Опционально.) Укажите ограничение для трафика всплеска (burst). Единица измерения – Кбайт.

По умолчанию

Ограничения не установлены.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Настроенное ограничение не должно превышать максимальную скорость на указанном интерфейсе. Если полученный трафик превышает заданное ограничение входящей полосы пропускания, отправляются кадры PAUSE или кадры Flow Control (управления потоком).

Пример

В данном примере показано, как настроить ограничения максимальной полосы пропускания на интерфейсе Ethernet 1/0/5. Заданные ограничения входящей полосы пропускания: 2000 Кбит/с и 4096 Кбайт для трафика всплеска (burst).

```
Switch#configure terminal
Switch(config)#interface eth1/0/5
Switch(config-if)#rate-limit input 2000 4096
Switch(config-if)#
```

52.14 service-policy

Данная команда используется для привязки карты политики к типу input или output на интерфейсе. Чтобы удалить политику обслуживания из входящего (input) или исходящего (output) интерфейса, воспользуйтесь формой **no** этой команды.

service-policy {input | output} *NAME*

no service-policy {input | output}

Параметры

input	Укажите, чтобы привязать карту политики к входящему потоку на интерфейсе.
output	Укажите, чтобы привязать карту политики к исходящему потоку на интерфейсе.
NAME	Укажите имя карты политики обслуживания. Максимальное количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Команда применима исключительно для настройки интерфейсов физического порта.

Используйте данную команду, чтобы привязать карту политики к типу input или output на интерфейсе. К каждому типу (input или output) может быть привязана только одна карта политики. Политика,

привязанная к интерфейсу, позволяет объединять и контролировать число или скорость пакетов. Поступающий на порт пакет будет обработан на основе политики обслуживания, привязанной к данному интерфейсу.

Пример

В данном примере показано, как создать карту политики «cust1-class» и привязать ее к интерфейсу Ethernet 1/0/1 для входящего трафика.

```
Switch#configure terminal
Switch(config)#policy-map cust1-classes
Switch(config-pmap)#exit
Switch(config)#interface eth1/0/1
Switch(config-if)#service-policy input cust1-classes
Switch(config-if)#
```

52.15 set

Данная команда используется для настройки полей нового приоритета (precedence), DSCP и CoS исходящего пакета. Также возможна настройка очереди CoS для пакета. Чтобы удалить заданные настройки, воспользуйтесь формой **no** этой команды.

set {[ip] precedence *PRECEDENCE* **| [ip] dscp** *DSCP* **| cos** *COS* **| cos-queue** *COS-QUEUE***}**
no set {[ip] precedence *PRECEDENCE* **| [ip] dscp** *DSCP* **| cos** *COS* **| cos-queue** *COS-QUEUE***}**

Параметры

precedence *PRECEDENCE*	Укажите новый приоритет пакета. Диапазон значений: от 0 до 7. Если указано ключевое слово **ip**, будет отмечен приоритет IPv4. Если не указано, будут отмечены приоритеты IPv4 и IPv6. Для пакетов IPv6 приоритетом являются три наиболее значимых бита класса трафика заголовка IPv6. Настройка приоритета не повлияет на выбор очереди CoS.
dscp *DSCP*	Укажите новый DSCP пакета. Диапазон значений: от 0 до 63. Если указано ключевое слово **ip**, будет отмечен IPv4 DSCP. Если не указано, будут отмечены IPv4 и IPv6 DSCP. Настройка DSCP не повлияет на выбор очереди CoS.
cos *COS*	Укажите новое значение CoS пакета. Диапазон значений: от 0 до 7.
cos-queue *COS-QUEUE*	Укажите очередь CoS для пакетов. Новое значение очереди CoS заменит первоначальное.

По умолчанию

Нет.

Режим ввода команды

Policy-map Class Configuration Mode.

Использование команды

Используйте данную команду для настройки полей нового приоритета (precedence), DSCP и CoS исходящего пакета. Введите команду **set cos-queue**, чтобы сразу же назначить очередь CoS для соответствующих пакетов.

Возможна настройка нескольких команд для класса, если они не конфликтуют.

Команда **set dscp** не повлияет на выбор очереди CoS. Команда **set cos-queue** не изменит поле CoS исходящего пакета.

Пример

В данном примере показано, как настроить карту политики «policy1» для класса «class1». Пакеты в указанном классе «class1» будут помечены DSCP 10.

```
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap-c)#
```

52.16 show class-map

Данная команда используется для отображения настроек карты класса.

show class-map [*NAME***]**

Параметры

NAME	(Опционально.) Укажите имя карты класса. Максимальное количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить все карты класса и их критерии соответствия.

Пример

В данном примере показано, как настроены две карты класса. Пакеты, соответствующие списку доступа «acl_home_user», принадлежат заданному классу «c3». IP-пакеты принадлежат настроенному классу «c2».

```
Switch#show class-map

Class Map match-any class-default
   Match any

 Class Map match-all c2
   Match protocol ip

Class Map match-all c3
   Match access-group acl_home_user

Switch#
```

52.17 show mls qos interface

Данная команда используется для отображения настроек уровня QoS на указанном интерфейсе.

show mls qos interface [*INTERFACE-ID* **[, | -]] {cos | scheduler | trust | rate-limit | queue-rate-limit | dscp-mutation | map {dscp-cos}}**

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
cos	Укажите, чтобы отобразить CoS по умолчанию.
scheduler	Укажите, чтобы отобразить настройки механизма обслуживания очереди передачи.
trust	Укажите, чтобы отобразить статус trust порта.
rate-limit	Укажите, чтобы отобразить ограничение полосы пропускания, настроенной для порта.
queue-rate-limit	Укажите, чтобы отобразить ограничение полосы пропускания, настроенной для очереди.
dscp-mutation	Укажите, чтобы отобразить карту DSCP Mutation, привязанную к интерфейсу.
map dscp-cos	Укажите, чтобы отобразить привязку DSCP к CoS.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если дополнительные параметры не указаны, отображается краткая информация о QoS. Когда в команде используется параметр **rate-limit** или **queue-rate-limit**, при отображении информации указываются проценты и фактическая скорость, если соединение порта активно. Если соединение порта неактивно, при отображении информации указываются только проценты.

Пример

В данном примере показано, как отобразить CoS по умолчанию для диапазона интерфейсов от Ethernet 1/0/2 до Ethernet 1/0/5.

```
Switch#show mls qos interface eth1/0/2-5 cos

 Interface     CoS   Override
 ------------  ----  ---------
 eth1/0/2      3     Yes
 eth1/0/3      4     No
 eth1/0/4      4     No
 eth1/0/5      3     No

Switch#
```

В примере ниже показано, как отобразить статус trust порта для диапазона интерфейсов от Ethernet 1/0/2 до Ethernet 1/0/5.

```
Switch#show mls qos interface eth1/0/2-5 trust

 Interface     Trust State
 ------------  ------------
 eth1/0/2      trust DSCP
 eth1/0/3      trust CoS
 eth1/0/4      trust DSCP
 eth1/0/5      trust CoS

Switch#
```

В следующем примере показано, как отобразить настройки механизма обслуживания очередей для интерфейсов Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch#show mls qos interface eth1/0/1-2 scheduler

 Interface     Scheduler Method
 ------------  -----------------
 eth1/0/1      sp
 eth1/0/2      wrr

Switch#
```

В нижеприведенном примере показано, как отобразить карты DSCP Mutation, которые привязаны к интерфейсам Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch#show mls qos interface eth1/0/1-2 dscp-mutation

 Interface     DSCP Mutation Map
 ------------  --------------------
 eth1/0/1      Mutate Map 1
 eth1/0/2      Mutate Map 2

Switch#
```

В нижеследующем примере показано, как отобразить ограничение полосы пропускания для диапазона интерфейсов от Ethernet 1/0/1 до Ethernet 1/0/4.

```
Switch#show mls qos interface eth1/0/1-4 rate-limit

 Interface Rx Rate             TX Rate             Rx Burst       Tx Burst
 --------- ------------------- ------------------- -------------- -------------
 eth1/0/1  1000 kbps           No Limit            64 kbyte       No Limit
 eth1/0/2  No Limit            2000 kbps           No Limit       2000 kbyte
 eth1/0/3  10%(100000 kbps)    20%(200000 kbps)    64 kbyte       64 kbyte
 eth1/0/4  2%                  2000 kbps           64 kbyte       64 kbyte

Switch#
```

В примере ниже показано, как отобразить ограничение полосы пропускания CoS для интерфейса Ethernet 1/0/1.

```
Switch#show mls qos interface Ethernet 1/0/1 queue-rate-limit


eth1/0/1
 QID   Min Bandwidth        Max Bandwidth
 ----  -------------------  -------------------
 0     No Limit             No Limit
 1     64 kbps              10%
 2     128 kbps             25600 kbps
 3     2%                   50%
 4     No Limit             No Limit
 5     No Limit             No Limit
 6     No Limit             No Limit
 7     No Limit             No Limit

Switch#
```

В нижеследующем примере показано, как отобразить привязку DSCP к CoS для интерфейса Ethernet 1/0/1.

```
Switch#show mls qos interface eth1/0/1 map dscp-cos

eth1/0/1
        0  1  2  3  4  5  6  7  8  9
      ---------------------------------
   00   00 00 00 00 00 00 00 00 01 01
   10   01 01 01 01 01 01 02 02 02 02
   20   02 02 02 02 03 03 03 03 03 03
   30   03 03 04 04 04 04 04 04 04 04
   40   05 05 05 05 05 05 05 05 06 06
   50   06 06 06 06 06 06 07 07 07 07
   60   07 07 07 07


Switch#
```

52.18 show mls qos map dscp-mutation

Данная команда используется для отображения настроек карты QoS DSCP Mutation.

show mls qos map dscp-mutation [*MAP-NAME***]**

Параметры

MAP-NAME	(Опционально.) Укажите имя карты DSCP Mutation для отображения.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения настроек карты QoS DSCP Mutation.

Пример

В данном примере показано, как отобразить карту DSCP Mutation глобально.

```
Switch# show mls qos map dscp-mutation

DSCP Mutation: mutemap1
Attaching interface:
   eth1/0/3

       0  1  2  3  4  5  6  7  8  9
     --------------------------------
   00  00 01 02 03 04 05 06 07 08 09
   10  10 11 12 13 14 15 16 17 18 19
   20  20 21 22 23 24 25 26 27 28 29
   30  08 31 32 33 34 35 36 37 38 39
   40  40 41 42 43 44 45 46 47 48 49
   50  50 51 52 53 54 55 56 57 58 59
   60  60 61 62 63


Switch#
```

52.19 show mls qos queueing

Данная команда используется, чтобы отобразить информацию об очередях QoS и настройках веса (weight) для разных алгоритмов обслуживания очередей на определенном интерфейсе или интерфейсах.

show mls qos queuing [interface I*NTERFACE-ID* [, | -]]

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить информацию об очередях QoS и настройках веса для разных алгоритмов обслуживания очередей на определенном интерфейсе или интерфейсах. Если **interface** не указан, отображается только системная карта привязки CoS к ID очереди.

Режим Scheduling, который настроен при помощи команды **mls qos scheduler**, определяет, какие настройки будут действовать для веса. Используйте команду **show mls qos interface scheduler**, чтобы отобразить настроенный алгоритм обслуживания очередей на интерфейсе.

Пример

В данном примере показано, как отобразить информацию об очередях QoS.

```
Switch#show mls qos queueing

 CoS-queue map:
   CoS    QID
   ---    ---
    0      2
    1      0
    2      1
    3      3
    4      4
    5      5
    6      6
    7      7


Switch#
```

В примере ниже показано, как отобразить настройки веса для разных алгоритмов обслуживания очередей на интерфейсе Ethernet 1/0/3.

```
Switch# show mls qos queueing interface eth1/0/3

wrr bandwidth weights:
  QID  Weights
  ---  -------
   0      1
   1      2
   2      3
   3      4
   4      5
   5      6
   6      7
   7      8

wdrr bandwidth weights:
  QID  Quantum
  ---  -------
   0      1
   1      2
   2      3
   3      4
   4      5
   5      6
   6      7
   7      8

Switch#
```

52.20 show policy-map

Данная команда используется для отображения настроек карты политики.

show policy-map [*POLICY-NAME* **| interface** *INTERFACE-ID***]**

Параметры

POLICY-NAME	(Опционально.) Укажите имя карты политики. Если не указано, будут отображены все карты политики.
interface *INTERFACE-ID*	(Опционально.) Укажите интерфейсы физического порта, которые необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить политики класса, настроенные для карты политики.

Пример

В данном примере показано, как отобразить политики класса, настроенные для карты политики.

```
Switch#show policy-map

 Policy Map cust1-classes
  Class Map gold


Switch#
```

52.21 wdrr-queue bandwidth

Данная команда используется, чтобы настроить значения quantum для очередей, обслуживаемых механизмом WDRR. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

wdrr-queue bandwidth *QUANTUM1...QUANTUM8*
no wdrr-queue bandwidth

Параметры

QUANTUM1 ...QUANTUM8	Укажите значение quantum (число длины кадров) для каждой из восьми очередей, обслуживаемых механизмом WDRR. Диапазон значений: от 0 до 127.

По умолчанию

Значение quantum для каждой очереди по умолчанию – 1.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Чтобы использовать данную команду, необходимо перейти в режим обслуживания очередей WDRR с помощью команды **mls qos scheduler wdrr**.

Пример

В данном примере показано, как настроить значения quantum для очередей в режиме обслуживания очередей WDRR на интерфейсе Ethernet 1/0/1. Для очереди 0 задано значение 1, для очереди 1 – 2, для очереди 2 – 3, для очереди 3 – 4, для очереди 5 – 6, для очереди 6 – 7 и для очереди 7 – 8.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mls qos scheduler wdrr
Switch(config-if)#wdrr-queue bandwidth 1 2 3 4 5 6 7 8
Switch(config-if)#
```

52.22 wrr-queue bandwidth

Данная команда позволяет указать/изменить полосу пропускания (bandwidth), предназначенную для очереди. Чтобы удалить полосу пропускания, предназначенную для очереди, воспользуйтесь формой **no** этой команды.

wrr-queue bandwidth *WEIGHT1...WEIGHT8*
no wrr-queue bandwidth

Параметры

WEIGHT1 ...WEIGHT8	Укажите значение веса (число кадров) для каждой очереди, обслуживаемой механизмом WRR. Диапазон значений: от 0 до 127.

По умолчанию

Значение веса для параметров от *WEIGHT1* до *WEIGHT7* по умолчанию – 1.
Значение веса для *WEIGHT8* по умолчанию – 0.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Чтобы применить данную команду, необходимо перейти в режим обслуживания очередей WRR с помощью команды **mls qos scheduler wrr**. При обслуживании Expedited Forwarding (EF) для очереди с наивысшим приоритетом всегда используется политика Per-hop Behavior (PHB) EF и настраивается режим обслуживания очередей по строгому приоритету (Strict Priority). При использовании Differentiate Service необходимо, чтобы вес последней очереди был равен нулю.

Пример

В данном примере показано, как настроить значения веса (weight) очередей в режиме обслуживания очередей WRR на интерфейсе Ethernet 1/0/1. Для очереди 0 задано значение 1, для очереди 1 – 2, для очереди 2 – 3, для очереди 3 – 4, для очереди 5 – 6, для очереди 6 – 7 и для очереди 7 – 8.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mls qos scheduler wrr
Switch(config-if)#wrr-queue bandwidth 1 2 3 4 5 6 7 8
Switch(config-if)#
```

53. Команды Remote Network MONitoring (RMON)

53.1 rmon collection stats

Данная команда используется для включения статистики RMON на настраиваемом интерфейсе. Чтобы отключить статистику, воспользуйтесь формой **no** этой команды.

rmon collection stats *INDEX* **[owner** *NAME***]**
no rmon collection stats *INDEX*

Параметры

INDEX	Укажите индекс таблицы RMON. Диапазон значений: от 1 до 65535.
owner *NAME*	Укажите имя владельца. Максимальное количество символов в строке – 127.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Номер записи группы статистики RMON является динамическим. Соответствующая запись в таблице будет доступна только на интерфейсе с включенной статистикой RMON.

Пример

В данном примере показано, как настроить запись статистики RMON на интерфейсе Ethernet 1/0/2. Индекс – 65. Имя владельца – guest.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#rmon collection stats 65 owner guest
Switch(config-if)#
```

53.2 rmon collection history

Данная команда используется для включения сбора истории статистики RMON MIB на настраиваемом интерфейсе. Чтобы отключить сбор истории статистики на интерфейсе, воспользуйтесь формой **no** этой команды.

rmon collection history *INDEX* **[owner** *NAME***] [buckets** *NUM***] [interval** *SECONDS***]**
no rmon collection history *INDEX*

Параметры

INDEX	Укажите индекс таблицы RMON. Диапазон значений: от 1 до 65535.

owner *NAME*	Укажите имя владельца. Максимальное количество символов в строке – 127.
buckets *NUM*	Укажите количество ячеек для сбора истории по группе статистики RMON. Диапазон значений: от 1 до 65535. Если не указано, используется значение по умолчанию – 50.
interval *SECONDS*	Укажите время в секундах для каждого цикла опроса (polling cycle). Диапазон значений: от 1 до 3600.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Номер записи группы статистики RMON является динамическим. Соответствующая запись в таблице будет доступна только на интерфейсе с включенной статистикой RMON. Настроенный интерфейс становится источником данных для созданной записи.

Пример

В данном примере показано, как включить сбор истории по группе статистики RMON MIB на интерфейсе Ethernet 1/0/8.

```
Switch#configure terminal
Switch(config)#interface eth1/0/8
Switch(config-if)#rmon collection history 101 owner it@domain.com interval 2000
Switch(config-if)#
```

53.3 rmon alarm

Данная команда используется для настройки записи уровня alarm (тревога) для мониторинга интерфейса. Чтобы удалить запись уровня alarm, воспользуйтесь формой **no** этой команды.

rmon alarm *INDEX VARIABLE INTERVAL* **{delta | absolute} rising-threshold** *VALUE* **[***RISING-EVENT-NUMBER***] falling-threshold** *VALUE* **[***FALLING-EVENT-NUMBER***] [owner** *STRING***]**

no rmon alarm *INDEX*

Параметры

INDEX	Укажите индекс alarm. Диапазон значений: от 1 до 65535.
VARIABLE	Укажите идентификатор объекта переменной для выборки.
INTERVAL	Укажите интервал в секундах для выборки переменной и проверки соответствия пороговых значений. Диапазон значений: от 1 до 2147483647.

delta	Укажите для мониторинга дельты (delta) двух последовательных значений выборки.
absolute	Укажите для мониторинга абсолютного значения выборки
rising-threshold *VALUE*	Укажите верхнее пороговое значение. Диапазон значений: от 0 до 2147483647.
RISING-EVENT-NUMBER	(Опционально.) Укажите индекс записи события, при котором превышено заданное верхнее пороговое значение. Диапазон значений: от 1 до 65535. Если не указано, никакие действия при превышении верхнего порогового значения не будут применены.
falling-threshold *VALUE*	Укажите нижнее пороговое значение. Диапазон значений: от 0 до 2147483647.
FALLING-EVENT-NUMBER	(Опционально.) Укажите индекс записи события, при котором достигнуто заданное нижнее пороговое значение. Диапазон значений: от 1 до 65535. Если не указано, никакие действия при достижении нижнего порогового значения не будут применены.
owner *STRING*	Укажите строку владельца. Максимально допустимое количество символов – 127.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

После настройки RMON alarm будут периодически производиться выборки переменных, значения которых будут проверены на соответствие настроенным пороговым значениям.

Пример

В данном примере показано, как настроить запись уровня alarm для мониторинга интерфейса.

```
Switch#configure terminal
Switch(config)#rmon alarm 783 1.3.6.1.2.1.2.2.1.12.6 30 delta rising-threshold 20 1 falling-
threshold 10 1 owner Name
Switch(config)#
```

53.4 rmon event

Данная команда используется для настройки записи события. Чтобы удалить запись события, воспользуйтесь формой **no** этой команды.

rmon event *INDEX* **[log] [[trap** *COMMUNITY***] [owner** *NAME***] [description** *TEXT***]**
no rmon event *INDEX*

Параметры

INDEX	Укажите индекс записи alarm. Доступный диапазон значений: от 1 до 65535.
log	(Опционально.) Укажите, чтобы генерировать сообщения в системном журнале для уведомлений.
trap *COMMUNITY*	(Опционально.) Укажите, чтобы генерировать сообщения SNMP trap для уведомлений. Максимальное количество символов – 127.
owner *NAME*	(Опционально.) Укажите имя владельца. Максимальное количество символов – 127.
description *TEXT*	(Опционально.) Укажите описание для записи события RMON. Максимальное количество символов в строке – 127.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Если указан параметр **log**, а **trap** не указан, при возникновении события генерируется запись в журнале. Если указан параметр **trap**, а **log** не указан, при возникновении события генерируется SNMP-уведомление.

Если указаны оба параметра (**log** и **trap**), при возникновении события генерируется и запись в журнале, и SNMP-уведомление.

Пример

В данном примере показано, как настроить генерирование записи в журнале при возникновении события. Индекс – 13.

```
Switch#configure terminal
Switch(config)#rmon event 13 log owner it@domain.com description ifInNUcastPkts is too much
Switch(config)#
```

53.5 show rmon alarm

Данная команда используется для отображения конфигурации alarm.

show rmon alarm

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить таблицу RMON alarm.

Пример

В данном примере показано, как отобразить таблицу RMON alarm.

```
Switch#show rmon alarm

Alarm index 23, owned by IT
  Monitors OID: 1.3.6.1.2.1.2.2.1.10.1
  every 120 second(s)
  Taking delta samples, last value was 2500
  Rising threshold is 2000, assigned to event 12
  Falling threshold is 1100, assigned to event 12
  On startup enable rising or falling alarm

Switch#
```

53.6 show rmon events

Данная команда используется для отображения таблицы событий RMON.

show rmon events

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить таблицу событий RMON.

Пример

В данном примере показано, как отобразить таблицу событий RMON.

```
Switch# show rmon events

Event 1, owned by manager1
  Description is Errors
  Event trigger action: log & trap sent to community manager
  Last triggered time: 13:12:15, 2020-03-12

Event 2, owned by manager2
  Description is Errors
  Event trigger action: log & trap
  Last triggered time: 0:0:0, 0

Switch#
```

53.7 show rmon history

Данная команда используется для отображения информации об истории статистики RMON.

show rmon history

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить историю статистики для всех настроенных записей.

Пример

В данном примере показано, как отобразить историю статистики RMON Ethernet.

```
Switch#show rmon history

Index 23, owned by Manager, Data source is eth1/0/2
  Interval: 30 seconds
  Requested buckets: 50, Granted buckets: 50
  Sample #1
    Received octets: 303595962, Received packets: 357568
    Broadcast packets: 3289, Multicast  packets: 7287
    Estimated utilization: 19
    Undersized packets: 213, Oversized  packets: 24
    Fragments: 2, Jabbers: 1
    CRC alignment errors: 0, Collisions: 0
  Drop events : 0
  Sample #2
    Received octets: 303596354, Received packets: 357898
    Broadcast packets: 3329, Multicast  packets: 7337
    Estimated utilization: 19
    Undersized packets: 213, Oversized  packets: 24
    Fragments: 2, Jabbers: 1
    CRC alignment errors: 0, Collisions: 0
  Drop events : 0

Switch#
```

53.8 show rmon statistics

Данная команда используется для отображения статистики RMON Ethernet.

show rmon statistics

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить статистику RMON Ethernet.

Пример

В данном примере показано, как отобразить статистику RMON Ethernet.

```
Switch#show rmon statistics

Index 32, owned by it@domain.com, Data Source is  eth1/0/3
  Received Octets : 234000, Received packets : 9706
  Broadcast packets: 2266, Multicast packets: 192
    Undersized packets: 213, Oversized  packets: 24
    Fragments: 2, Jabbers: 1
    CRC alignment errors: 0, Collisions: 0
  Drop events : 0
  Packets in 64 octets: 256, Packets in 65-127 octets : 236
  Packets in 128-255 octets : 129, Packets in 256-511 octets : 10
  Packets in 512-1023 octets : 38, Packets in 1024-1518 octets : 2200

Switch#
```

53.9 snmp-server enable traps rmon

Данная команда используется для включения отправки SNMP-уведомлений для RMON. Чтобы отключить отправку SNMP-уведомлений для RMON, воспользуйтесь формой **no** этой команды.

snmp-server enable traps rmon [rising-alarm | falling-alarm]

no snmp-server enable traps rmon [rising-alarm | falling-alarm]

Параметры

rising-alarm	(Опционально.) Укажите, чтобы настроить отправку trap, уведомляющих о поднятии тревоги.
falling-alarm	(Опционально.) Укажите, чтобы настроить отправку trap, уведомляющих об отмене тревоги.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы включить/отключить отправку SNMP-уведомлений для RMON.

Пример

В данном примере показано, как включить отправку RMON trap, уведомляющих о поднятии и об отмене тревоги.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps rmon
Switch(config)#
```

54. Команды Router Advertisement (RA) Guard

54.1 ipv6 nd raguard policy

Данная команда используется для создания политики Router Advertisement (RA) Guard Policy и для входа в режим RA Guard Policy Configuration Mode. Чтобы удалить политику RA Guard Policy, воспользуйтесь формой **no** этой команды.

ipv6 nd raguard policy *POLICY-NAME*
no ipv6 nd raguard policy *POLICY-NAME*

Параметры

POLICY-NAME	Укажите имя политики IPv6 RA Guard Policy.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы создать политику RA Guard Policy и войти в режим RA Guard Policy Configuration Mode.

Пример

В данном примере показано, как создать политику RA Guard Policy под именем «policy1».

```
Switch#configure terminal
Switch(config)#ipv6 nd raguard policy policy1
Switch(config-ra-guard)#
```

54.2 device-role

Данная команда используется для настройки роли подключенного устройства. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

device-role {host | router}
no device-role

Параметры

host	Укажите, чтобы настроить подключенное устройство в качестве узла.
router	Укажите, чтобы настроить подключенное устройство в качестве маршрутизатора.

По умолчанию

Роль по умолчанию – **host**.

Режим ввода команды

RA Guard Policy Configuration Mode.

Использование команды

Используйте данную команду, чтобы указать роль подключенного устройства. Так как по умолчанию устройство выполняет роль узла, получаемые Router Advertisement (RA) и сообщения переадресации будут заблокированы. Если устройство настроено в качестве маршрутизатора, Router Solicitation (RS), Router Advertisement (RA) и сообщения переадресации будут разрешены на данном порту.

Пример

В данном примере показано, как создать политику RA Guard Policy под именем «raguard1» и настроить устройство в качестве узла.

```
Switch#configure terminal
Switch(config)#ipv6 nd raguard policy raguard1
Switch(config-ra-guard)#device-role host
Switch(config-ra-guard)#
```

54.3 match ipv6 access-list

Данная команда используется для фильтрации RA-сообщений на основе IPv6-адреса отправителя. Чтобы отключить фильтрацию, воспользуйтесь формой **no** этой команды.

match ipv6 access-list *IPV6-ACCESS-LIST-NAME*
no match ipv6 access-list

Параметры

IPV6-ACCESS-LIST-NAME	Укажите стандартный список доступа IPv6.

По умолчанию

Нет.

Режим ввода команды

RA Guard Policy Configuration Mode.

Использование команды

Используйте данную команду для устройства в роли маршрутизатора (router), чтобы отфильтровать RA-сообщения на основе IP-адреса отправителя. Если команда **match ipv6 access-list** не настроена, все RA-сообщения будут игнорироваться. Список доступа настраивается с помощью команды **ipv6 access-list**.

Пример

В данном примере показано, как создать политику RA Guard Policy и настроить проверку соответствия IPv6-адресов списку доступа «list1».

```
Switch#configure terminal
Switch(config)#ipv6 nd raguard policy raguard1
Switch(config-ra-guard)#match ipv6 access-list list1
Switch(config-ra-guard)#
```

54.4 ipv6 nd raguard attach-policy

Данная команда используется для применения политики RA Guard Policy на определенном интерфейсе. Чтобы удалить привязку, воспользуйтесь формой **no** этой команды.

ipv6 nd raguard attach-policy [*POLICY-NAME***]**

no ipv6 nd raguard

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики RA Guard Policy.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Может быть применена только одна политика RA Policy. Если имя политики не указано, политика по умолчанию настроит устройство в качестве узла.

Пример

В данном примере показано, как применить политику RA Guard Policy на интерфейсе Ethernet 1/0/3.

```
Switch# configure terminal
Switch(config)# ipv6 nd raguard policy raguard1
Switch(config-ra-guard)# device-role router
Switch(config-ra-guard)# match ipv6 access-list list1
Switch(config-ra-guard)# exit
Switch(config)# interface eth1/0/3
Switch(config-if)# ipv6 nd raguard attach-policy raguard1
Switch(config-if)#
```

54.5 show ipv6 nd raguard policy

Данная команда используется для отображения информации о политике IPv6 RA Guard Policy.

show ipv6 nd raguard policy [*POLICY-NAME***]**

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики IPv6 RA Guard Policy.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить информацию о политике RA Guard Policy. Если параметры не указаны, будет отображена информация для всех политик.

Пример

В данном примере показано, как отобразить информацию о политике RA Guard Policy «raguard1».

```
Switch# show ipv6 nd raguard policy raguard1

Policy raguard1 configuration:
      Device Role: host
      Target: eth1/0/1-1/0/2

Switch#
```

55. Команды Safeguard Engine

55.1 clear cpu-protect counters

Данная команда используется для обнуления счетчиков защиты ЦПУ.

clear cpu-protect counters {all | sub-interface [manage | protocol | route] | type [*PROTOCOL-NAME***]}**

Параметры

all	Укажите для обнуления всех счетчиков защиты ЦПУ.
sub-interface [manage | protocol | route]	Укажите для обнуления счетчиков защиты ЦПУ под-интерфейсов. Если под-интерфейс не указан, будут обнулены счетчики защиты ЦПУ всех под-интерфейсов.
type [*PROTOCOL-NAME*]	Укажите для обнуления счетчиков защиты ЦПУ определенного протокола. Если имя протокола не указано, будут обнулены счетчики защиты ЦПУ всех протоколов.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

При вводе команды без параметров будут обнулены все счетчики защиты ЦПУ.

Пример

В данном примере показано, как удалить всю статистику защиты ЦПУ.

```
Switch#clear cpu-protect counters all
Switch#
```

55.2 cpu-protect safeguard

Данная команда используется для включения или настройки функции Safeguard Engine. Для выключения функции Safeguard Engine воспользуйтесь формой **no** этой команды.

cpu-protect safeguard [threshold *RISING-THRESHOLD FALLING-THRESHOLD***]**

no cpu-protect safeguard [threshold]

Параметры

threshold	(Опционально.) Укажите, чтобы настроить пороговые значения загрузки, при которой будет включаться/отключаться функция Safeguard Engine.

RISING-THRESHOLD	(Опционально.) Укажите, чтобы установить значение в процентах верхнего порога загрузки ЦПУ, при котором включается функция Safeguard Engine. Если загрузка ЦПУ превысит указанное значение, механизм Safeguard Engine начнет функционировать. Диапазон значений: от 20 до 100.
FALLING-THRESHOLD	(Опционально.) Укажите, чтобы установить значение в процентах нижнего порога загрузки ЦПУ, при котором выключается функция Safeguard Engine. Если загрузка ЦПУ снизится до указанного значения, механизм Safeguard Engine перестанет функционировать. Диапазон значений: от 20 до 100.

По умолчанию

По умолчанию функция Safeguard Engine отключена.
Верхний порог загрузки ЦПУ по умолчанию – 50.
Нижний порог загрузки ЦПУ по умолчанию – 20.

Режим ввода команды

Global Configuration Mode.

Использование команды

Safeguard Engine позволяет сохранить устройство в работоспособном состоянии при атаке, минимизируя рабочую загрузку коммутатора и одновременно давая возможность пересылать важные пакеты по сети в ограниченной полосе пропускания. Если загрузка ЦПУ превышает установленный верхний порог, коммутатор переходит в режим высокой загрузки (Exhausted Mode). В данном режиме коммутатор ограничивает полосу пропускания принимаемых ARP-пакетов и широковещательных IP-пакетов.

Пример

В данном примере показано, как включить Safeguard Engine и настроить пороговые значения. Верхнее пороговое значение – 60. Нижнее пороговое значение – 40.

```
Switch#configure terminal
Switch(config)#cpu-protect safeguard threshold 60 40
Switch(config)#
```

55.3 cpu-protect sub-interface

Данная команда используется для настройки пропускной способности (Rate Limit) трафика, предназначенного для ЦПУ по типам под-интерфейсов. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

cpu-protect sub-interface {manage | protocol | route} pps *RATE*
no cpu-protect sub-interface {manage | protocol | route}

Параметры

RATE	Укажите пороговое значение. Единица измерения – пакеты в секунду. Если установлено значение 0, будут отброшены все пакеты указанных типов под-интерфейса.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Причины, по которым пакеты предназначаются для ЦПУ, могут быть классифицированы по следующим трем группам: **manage**, **protocol** и **route**. Под-интерфейс – это логический интерфейс, предназначенный для разделения полученных пакетов ЦПУ на разные группы. Как правило, для корректной работы функций пакеты протокола должны иметь более высокий приоритет. Обычно ЦПУ не участвует в маршрутизации пакетов. В некоторых случаях, например, при изучении нового IP-адреса, или если не указан маршрут по умолчанию, некоторые пакеты будут оправлены в ЦПУ для программной маршрутизации. Используйте данную команду, чтобы ограничить скорость маршрутизируемых пакетов. Это позволит ЦПУ не тратить много времени на маршрутизацию пакетов.

Пример

В данном примере показано, как настроить пропускную способность (Rate Limit) пакетов для под-интерфейса управления (management). Настроенное пороговое значение – 1000 пакетов в секунду.

```
Switch# configure terminal
Switch(config)# cpu-protect sub-interface manage pps 1000
Switch(config)#
```

55.4 cpu-protect type

Данная команда используется для настройки пропускной способности (Rate Limit) трафика, предназначенного для ЦПУ, по типу протокола. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

cpu-protect type *PROTOCOL-NAME* **pps** *RATE*

no cpu-protect type *PROTOCOL-NAME*

Параметры

PROTOCOL-NAME	Укажите имя протокола, который необходимо настроить.
RATE	Укажите пороговое значение. Единица измерения – пакеты в секунду. Если установлено значение 0, будут отброшены все пакеты указанного протокола.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

ЦПУ должно обрабатывать следующие пакеты: протоколы маршрутизации, протоколы 2 уровня и пакеты для управления. ЦПУ, перегруженное предназначенным для него трафиком, будет тратить много времени на обработку ненужного трафика, что повлияет на процессы маршрутизации. Чтобы уменьшить нагрузку на ЦПУ, используйте данную команду для настройки порогового значения пакетов указанного протокола.

В соответствии с назначением пакетов, предназначенных для ЦПУ, маршрутизатор создает три виртуальных под-интерфейса для обработки пакетов:

- **manage** – пакеты предназначены для любого интерфейса маршрутизатора или интерфейса системы управления сетью через протокол интерактивного доступа, такого как Telnet или SSH;
- **protocol** – пакеты управления протоколом, которые могут быть идентифицированы маршрутизатором;
- **route** – другие пакеты, поступающие на маршрутизатор для маршрутизации, которые должны быть обработаны ЦПУ, прежде чем это будет сделано без участия ЦПУ.

В таблице ниже перечислены имена поддерживаемых протоколов для данной команды:

Имя протокола	Описание	Классификация (под-интерфейс)
8021x	Port-based Network Access Control	Protocol
arp	IP Address Resolution Protocol (ARP)	Protocol
dhcp	Dynamic Host Configuration	Protocol
dns	Domain Name Services	Protocol
icmpv4	IPv4 Internet Control Message Protocol	Protocol
icmpv6-nighbor	IPv6 ICMP Neighbor Discover Protocol (NS/NA/RS/RA)	Protocol
icmpv6-other	IPv6 ICMP except NDP NS/NA/RS/RA	Protocol
igmp	Internet Group Management Protocol	Protocol
lacp	Link Aggregation Control Protocol	Protocol
snmp	Simple Network Management Protocol	Manage
ssh	Secured shell	Manage
stp	Spanning Tree Protocol (802.1D)	Protocol
telnet	Telnet	Manage
tftp	Trivial File Transfer Protocol	Manage

web	HTTP and HTTPS	Manage

Пример

В данном примере показано, как настроить пороговое значение пакетов протокола ARP. Настроенное пороговое значение – 100 пакетов в секунду.

```
Switch#configure terminal
Switch(config)# cpu-protect type arp pps 100
Switch(config)#
```

55.5 show cpu-protect safeguard

Данная команда используется для отображения настроек и статуса функции Safeguard Engine.

show cpu-protect safeguard

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить настройки и статус функции Safeguard Engine.

Пример

В данном примере показано, как отобразить настройки и текущий статус Safeguard Engine.

```
Switch#show cpu-protect safeguard

Safeguard Engine State: Disabled
Safeguard Engine Status: Normal
Utilization Thresholds:
 Rising   :30%
 Falling  :20%

Switch#
```

Отображаемые параметры

Safeguard Engine Status	Текущий режим загрузки ЦПУ. Возможны следующие строки для отображения: **Exhausted**: если загрузка ЦПУ превышает установленный верхний порог, коммутатор переходит в режим Exhausted Mode, и механизм

	Safeguard Engine начинает функционировать. Safeguard Engine не выключается до тех пор, пока загрузка не снизится до нижнего порога. **Normal**: Safeguard Engine не срабатывает.

55.6 show cpu-protect sub-interface

Данная команда используется для отображения пропускной способности (Rate Limit) и статистики под-интерфейса.

show cpu-protect sub-interface {manage | protocol | route}

Параметры

manage	Укажите под-интерфейс менеджера, который необходимо отобразить.
protocol	Укажите под-интерфейс протокола, который необходимо отобразить.
route	Укажите под-интерфейс маршрута, который необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить настроенные значения Rate Limit и Drop Count механизма Safeguard Engine указанной группы. Данные счетчики подсчитываются программно.

Пример

В данном примере показано, как отобразить настроенные значения Rate Limit и Drop Count механизма Safeguard Engine указанной группы.

```
Switch#show cpu-protect sub-interface manage

Sub-Interface: manage
Rate Limit: N/A

Switch#
```

55.7 show cpu-protect type

Данная команда используется для отображения пропускной способности (Rate Limit) и статистики защиты ЦПУ.

show cpu-protect type *PROTOCOL-NAME*

Параметры

PROTOCOL-NAME	Укажите для отображения настроенного значения Rate Limit и статистики указанного протокола.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить Rate Limit и статистику механизма Safeguard Engine.

Пример

В данном примере показано, как отобразить Rate Limit и статистику механизма Safeguard Engine.

```
Switch#show cpu-protect type arp

Type: arp
Rate Limit: N/A

Switch#
```

55.8 snmp-server enable traps safeguard-engine

Данная команда используется для включения отправки SNMP-уведомлений для Safeguard Engine. Для отключения отправки SNMP-уведомлений для Safeguard Engine воспользуйтесь формой **no** этой команды.

snmp-server enable traps safeguard-engine

no snmp-server enable traps safeguard-engine

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы включить/отключить отправку SNMP-уведомлений для Safeguard Engine.

Пример

В данном примере показано, как включить отправку SNMP-уведомлений для Safeguard Engine.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps safeguard-engine
Switch(config)#
```

56. Команды Secure Shell (SSH)

56.1 crypto key generate

Данная команда используется для генерирования пары ключей RSA или DSA.

crypto key generate {rsa [modulus *MODULUS-SIZE*] **| dsa}**

Параметры

rsa	Укажите для генерирования пары ключей RSA.
modulus *MODULUS-SIZE*	(Опционально.) Укажите количество битов в модуле. Доступные значения для RSA: 360, 512, 768, 1024 и 2048. Если не указано, будет получено сообщение о необходимости указать значение.
dsa	Укажите для генерирования пары ключей DSA. Фиксированный размер ключа DSA – 1024 битов.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для генерирования пары ключей RSA или DSA.

Пример

В данном примере показано, как создать ключ RSA.

```
Switch#crypto key generate rsa

The RSA key pairs already existed.
Do you really want to replace them? (y/n) [n]y
Choose the size of the key modulus in the range of 360 to 2048.The process may take
a few minutes.
Number of bits in the modulus [768]: 768
Generating RSA key...Done

Switch#
```

56.2 crypto key zeroize

Данная команда используется для удаления пары ключей RSA или DSA.

crypto key zeroize {rsa | dsa}

Параметры

rsa	Укажите, чтобы удалить пару ключей RSA.
dsa	Укажите, чтобы удалить пару ключей DSA.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы удалить пару открытых ключей SSH-сервера. Если обе пары ключей RSA и DSA удалены, SSH-сервер будет недоступен.

Пример

В данном примере показано, как удалить ключ RSA.

```
Switch#crypto key zeroize rsa

Do you really want to remove the key? (y/n)[n]: y

Switch#
```

56.3 ip ssh timeout

Данная команда используется для настройки параметров контроля SSH на коммутаторе. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip ssh {timeout *SECONDS* **| authentication-retries** *NUMBER***}**
no ip ssh {timeout | authentication-retries}

Параметры

timeout *SECONDS*	Укажите временной интервал ожидания ответа от SSH-клиента для этапа согласования SSH. Диапазон значений: от 30 до 600.
authentication-retries *NUMBER*	Укажите количество попыток аутентификации. Сессия завершается после всех неудачных попыток. Диапазон значений: от 1 до 32.

По умолчанию

По умолчанию значение тайм-аута – 120 секунд.
По умолчанию количество попыток аутентификации – 3.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить параметры SSH-сервера на коммутаторе. С помощью параметра **authentication-retries** укажите максимальное количество попыток аутентификации перед завершением сессии.

Пример

В данном примере показано, как настроить значение тайм-аута для SSH. Указанное значение – 160 секунд.

```
Switch#configure terminal
Switch(config)#ip ssh timeout 160
Switch(config)#
```

В примере ниже показано, как настроить значение попыток аутентификации. Указанное значение – 2. Соединение будет прервано после 2 неудачных попыток.

```
Switch#configure terminal
Switch(config)#ip ssh authentication-retries 2
Switch(config)#
```

56.4 ip ssh server

Данная команда используется для включения SSH-сервера. Чтобы отключить SSH-сервер, воспользуйтесь формой **no** этой команды.

ip ssh server

no ip ssh server

Параметры

Нет.

По умолчанию

По умолчанию SSH-сервер отключен.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы включить/отключить SSH-сервер.

Пример

В данном примере показано, как включить SSH-сервер.

```
Switch#configure terminal
Switch(config)#ip ssh server
Switch(config)#
```

56.5 ip ssh service-port

Данная команда используется для указания сервисного порта для SSH. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip ssh service-port *TCP-PORT*
no ip ssh service-port

Параметры

TCP-PORT	Укажите номер TCP-порта. Диапазон значений: от 1 до 65535. Как правило, для протокола SSH назначается TCP-порт 22.

По умолчанию

По умолчанию номер TCP-порта – 22.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить номер TCP-порта для SSH-сервера.

Пример

В данном примере показано, как изменить номер сервисного порта. Новый настроенный номер – 3000.

```
Switch#configure terminal
Switch(config)#ip ssh service-port 3000
Switch(config)#
```

56.6 show crypto key mypubkey

Данная команда используется для отображения пар открытых ключей RSA или DSA.

show crypto key mypubkey {rsa | dsa}

Параметры

rsa	Укажите, чтобы отобразить информацию об открытом ключе RSA.
dsa	Укажите, чтобы отобразить информацию об открытом ключе DSA.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить пары открытых ключей RSA или DSA.

Пример

В данном примере показано, как отобразить информацию об открытом ключе RSA.

```
Switch#show crypto key mypubkey rsa

% Key pair was generated at: 09:48:40, 2013-11-29
Key Size: 768 bits
Key Data:
AAAAB3Nz aC1yc2EA AADAQAB AAAAQwCN 6IRFHCBf jsHvYjQG iCL0p2kz 2v38ULC8
kAKra/Ze mG7IW3eC 8STcrkr5 s7l9H/bh jG/oqkwj SlUJSGqR e/sj6Ws=

Switch#
```

56.7 show ip ssh

Данная команда используется для отображения пользовательских настроек конфигурации SSH.

show ip ssh

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить настройки конфигурации SSH.

Пример

В данном примере показано, как отобразить настройки конфигурации SSH.

```
Switch#show ip ssh

IP SSH server             : Enabled
IP SSH service port       : 22
SSH server mode           : V2
Authentication timeout    : 120 secs
Authentication retries    : 3 times

Switch#
```

56.8 show ssh

Данная команда используется для отображения статуса подключений SSH-сервера.

show ssh

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить статус подключений SSH на коммутаторе.

Пример

В данном примере показано, как отобразить информацию о подключениях SSH.

```
Switch#show ssh

SID Ver. Cipher                       Userid           Client IP Address
--- --- ----------------------------- ---------------- -------------------------
0   V2  3des-cbc/hmac-sha1-96         zhang3           192.168.0.100
1   V2  3des-cbc/hmac-sha1            lee4567890123456 2000::243

Total Entries: 2

Switch#
```

Отображаемые параметры

SID	Уникальный номер, идентифицирующий сессию SSH.
Ver	Версия SSH указанной сессии.
Cipher	Криптографический/Hashed Message Authentication Code (HMAC) алгоритм, используемый SSH-клиентом.
Userid	Имя пользователя сессии.
Client IP Address	IP-адрес клиента для установленной сессии SSH.

56.9 ssh user authentication-method

Данная команда используется для настройки методов аутентификации SSH для учетной записи пользователя. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ssh user *NAME* **authentication-method {password | publickey** *URL* **| hostbased** *URL* **host-name** *HOSTNAME* **[***IP-ADDRESS* **|** *IPV6-ADDRESS***]}**

no ssh user *NAME* **authentication-method**

Параметры

NAME	Укажите имя пользователя для настройки типа аутентификации. Имя пользователя должно быть существующей локальной учетной записью. Максимальное количество символов – 32.
password	Укажите метод аутентификации по паролю для указанной учетной записи пользователя. Данный метод аутентификации используется по умолчанию.
publickey *URL*	Укажите метод аутентификации с открытым ключом для указанной учетной записи пользователя. Введите URL локального файла, который будет использоваться в качестве открытого ключа указанного пользователя.
hostbased *URL*	Укажите метод аутентификации на основе узла для указанной учетной записи пользователя. Введите URL локального файла, который будет использоваться в качестве ключа узла клиента.
host-name *HOSTNAME*	Укажите доступное имя узла для аутентификации на основе узла. Имя узла клиента проверяется во время аутентификации. Диапазон значений: от 1 до 255.
IP-ADDRESS	(Опционально.) Укажите, необходима ли дополнительная проверка IP-адреса клиента для аутентификации на основе узла. Если не указано, будет проверено только имя узла.
IPV6-ADDRESS	(Опционально.) Укажите, необходима ли дополнительная проверка IPv6-адреса клиента для аутентификации на основе узла. Если не указано, будет проверено только имя узла.

По умолчанию

По умолчанию используется метод аутентификации по паролю.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить метод аутентификации для пользователя. Имя пользователя должно быть пользователем, созданным при помощи команды **username**. По умолчанию используется метод аутентификации по паролю. Системой будет предложено ввести пароль.

Для аутентификации пользователя при помощи открытого ключа SSH скопируйте файл открытого ключа пользователя в файловую систему. Когда пользователь пытается войти в учетную запись на коммутаторе через SSH-клиента (используя метод открытого ключа SSH), SSH-клиент автоматически передаст коммутатору открытый ключ и подпись с закрытым ключом. Если и открытый ключ, и

подпись верны, пользователь будет аутентифицирован, и вход в учетную запись коммутатора будет разрешен.

Для аутентификации пользователя при помощи открытого ключа SSH или метода на основе узла необходимо указать файл открытого ключа пользователя или файл ключа узла клиента в одном и том же формате. Файл ключа может содержать несколько ключей. Каждый ключ должен быть определен одной строкой. Максимальная длина строки составляет 8 Kb.

Каждый ключ состоит из следующих разделенных пробелами полей: *keytype*, *base64-encoded key*, *comment*. Ввод полей *keytype* и *base64-encoded key* обязателен, ввод поля *comment* –необязатетелен. Поле *keytype* может являться *ssh-dss* или *ssh-rsa*.

Пример

В данном примере показано, как настроить метод аутентификации с открытым ключом для пользователя «user1».

```
Switch# configure terminal
Switch(config)# ssh user tom authentication-method publickey c:/user1.pub
Switch(config)#
```

57. Команды Simple Network Management Protocol (SNMP)

57.1 show snmp trap link-status

Данная команда используется для отображения состояния trap-статуса канала на интерфейсе.

show snmp trap link-status [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения состояния trap-статуса при обнаружении/разрыве соединения (link-up / link-down) на интерфейсе. Если параметры не указаны, будут отображены все интерфейсы.

Пример

В данном примере показано, как отобразить trap-статус соединения для диапазона интерфейсов от Ethernet 1/0/1 до Ethernet 1/0/9.

```
Switch#show snmp trap link-status interface eth1/0/1-9

Interface           Trap state
-------------       -------------
eth1/0/1            Enabled
eth1/0/2            Enabled
eth1/0/3            Enabled
eth1/0/4            Enabled
eth1/0/5            Enabled
eth1/0/6            Enabled
eth1/0/7            Enabled
eth1/0/8            Enabled
eth1/0/9            Enabled


Switch#
```

57.2 show snmp-server

Данная команда используется для отображения глобальных настроек о состоянии SNMP-сервера и настроек, касающихся состояния trap.

show snmp-server [traps]

Параметры

traps	(Опционально.) Укажите для отображения настроек, касающихся состояния trap.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Для отображения глобальных настроек о состоянии SNMP-сервера используйте команду **show snmp-server.**

Для отображения настроек, касающихся состояния trap, введите команду **show snmp-server traps.**

Пример

В данном примере показано, как отобразить настройки SNMP-сервера.

```
Switch# show snmp-server

SNMP Server  : Enabled
Name         : SiteA-Switch
Location     : HQ 15F
Contact      : MIS Department II
SNMP UDP Port: 50000
SNMP Response Broadcast Request: Enabled

Switch#
```

В примере ниже показано, как отобразить настройки, касающиеся состояния trap.

```
Switch# show snmp-server traps

Global Trap State : Enabled
Individual Trap State:
  Authentication          : Enabled
  linkup                  : Enabled
  linkdown                : Enabled
  coldstart               : Enabled
  warmstart               : Disabled

Switch#
```

57.3 show snmp-server trap-sending

Данная команда используется для отображения состояния отправки SNMP trap на порту.

show snmp-server trap-sending [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить состояние отправки SNMP trap на порту. Если параметры не указаны, будут отображены все порты.

Пример

В данном примере показано, как отобразить состояние отправки SNMP trap для диапазона интерфейсов от Ethernet 1/0/1 до Ethernet 1/0/9.

```
Switch# show snmp-server trap-sending interface eth1/0/1-9

      Port                          Trap Sending
-----------------                 ---------------
 eth1/0/1                            Enabled
 eth1/0/2                            Enabled
 eth1/0/3                            Disabled
 eth1/0/4                            Enabled
 eth1/0/5                            Enabled
 eth1/0/6                            Disabled
 eth1/0/7                            Enabled
 eth1/0/8                            Enabled
 eth1/0/9                            Enabled

Switch#
```

57.4 snmp-server

Данная команда используется для включения агента SNMP. Чтобы выключить агента SNMP, воспользуйтесь формой **no** этой команды.

snmp-server
no snmp-server

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Менеджер SNMP управляет агентом SNMP: отправляет SNMP-запросы агенту и получает ответы и SNMP-уведомления от агента. Для управления агентом необходимо включить на нем SNMP-серевер.

Пример

В данном примере показано, как включить SNMP-сервер.

```
Switch#configure terminal
Switch(config)#snmp-server
Switch(config)#
```

57.5 snmp-server contact

Данная команда используется, чтобы настроить системную контактную информацию для устройства. Для удаления настроек воспользуйтесь формой no этой команды.

snmp-server contact *TEXT*
no snmp-server contact

Параметры

TEXT	Укажите системную контактную информацию. Максимальное количество символов в строке – 255. Пробелы в строке допустимы.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить системную контактную информацию для управления устройством.

Пример

В данном примере показано, как указать строку с системной контактной информацией. Настроенная строка – MIS Department II.

```
Switch#configure terminal
Switch(config)#snmp-server contact MIS Department II
Switch(config)#
```

57.6 snmp-server enable traps

Данная команда используется для глобального включения отправки SNMP trap. Чтобы отключить отправку SNMP trap, воспользуйтесь формой **no** этой команды.

snmp-server enable traps
no snmp-server enable traps

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы включить/отключить отправку SNMP trap глобально на устройстве.

Пример

В данном примере показано, как включить отправку SNMP trap глобально.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps
Switch(config)#
```

57.7 snmp-server enable traps snmp

Данная команда используется для включения отправки всех или определенных SNMP-уведомлений. Чтобы отключить отправку всех или определенных SNMP-уведомлений, воспользуйтесь формой **no** этой команды.

snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]

no snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]

Параметры

authentication	(Опционально.) Укажите для отправки SNMP trap об ошибке аутентификации. Trap-сообщение «authenticationFailuretrap» генерируется, если устройство получает SNMP-сообщение, которое не аутентифицировано должным образом. Метод аутентификации зависит от используемой версии SNMP. При использовании SNMPv1 или SNMPv2c ошибка аутентификации возникает, если пакеты были сформированы с указанием неверной строки сообщества (community string). При использовании SNMPv3 ошибка аутентификации возникает, если пакеты были сформированы с указанием неверного ключа аутентификации SHA/MD5.
linkup	(Опционально.) Укажите для отправки SNMP-уведомлений об установленном соединении. Trap-сообщение «linkUp (3)» генерируется, если на устройстве установлено соединение хотя бы с одним из каналов связи.
linkdown	(Опционально.) Укажите для отправки SNMP-уведомлений о прерванном соединении. Trap-сообщение «linkDown (2)» генерируется, если на устройстве прервано соединение хотя бы с одним из каналов связи.

coldstart	(Опционально.) Укажите для отправки SNMP-уведомлений о «холодном» старте.
warmstart	(Опционально.) Укажите для отправки SNMP-уведомлений о «горячем» старте.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду для управления отправкой стандартных SNMP trap. Чтобы включить отправку SNMP-trap, необходимо также включить этот параметр глобально.

Пример

В данном примере показано, как включить отправку всех SNMP trap на узел 10.9.18.100, используя строку сообщества «public».

```
Switch#configure terminal
Switch(config)#snmp-server enable traps
Switch(config)#snmp-server enable traps snmp
Switch(config)#snmp-server host 10.9.18.100 version 2c public
Switch(config)#
```

В примере ниже показано, как включить SNMP trap об ошибке аутентификации.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps snmp authentication
Switch(config)#
```

57.8 snmp-server location

Данная команда используется для указания информации о системном местоположении. Чтобы удалить настройки, воспользуйтесь формой **no** этой команды.

snmp-server location *TEXT*

no snmp-server location

Параметры

TEXT	Укажите системное местоположение. Максимальное количество символов в строке – 255. Пробелы в строке допустимы.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду для указания информации о системном местоположении на коммутаторе.

Пример

В данном примере показано, как указать строку с информацией о системном местоположении. Указанная строка – HQ 15F.

```
Switch#configure terminal
Switch(config)#snmp-server location HQ 15F
Switch(config)#
```

57.9 snmp-server name

Данная команда используется для указания информации о системном имени. Чтобы удалить настройки, воспользуйтесь формой **no** этой команды.

snmp-server name *NAME*

no snmp-server name

Параметры

NAME	Укажите имя сервера. Максимальное количество символов в строке – 255. Оптимальное количество символов в строке – не более 10.

По умолчанию

Имя по умолчанию – Switch.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду для указания информации о системном имени коммутатора.

Пример

В данном примере показано, как настроить системное имя. Указанное имя – SiteA-switch.

```
Switch#configure terminal
Switch(config)#snmp-server name SiteA-switch
SiteA-switch(config)#
```

57.10 snmp-server trap-sending disable

Данная команда используется для отключения отправки SNMP trap на порту. Чтобы включить отправку SNMP trap на порту, воспользуйтесь формой **no** этой команды.

snmp-server trap-sending disable
no snmp-server trap-sending disable

Параметры

Нет.

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Используйте данную команду, чтобы включить/отключить отправку сгенерированных системой SNMP trap с определенного порта. Данная команда не применима для SNMP trap, сгенерированных другой системой и переадресованных на порт.

Пример

В данном примере показано, как отключить отправку SNMP trap на интерфейсе с интерфейса Ethernet 1/0/8.

```
Switch#configure terminal
Switch(config)#interface eth1/0/8
Switch(config-if)#snmp-server trap-sending disable
Switch(config-if)#
```

57.11 snmp-server service-port

Данная команда используется для настройки номера UDP-порта SNMP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

snmp-server service-port *PORT-NUMBER*
no snmp-server service-port

Параметры

PORT-NUMBER	Укажите номер UDP-порта. Диапазон значений: от 1 до 65535. Некоторые номера могут конфликтовать с другими протоколами.

По умолчанию

Номер по умолчанию – 161.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду для настройки номера UDP-порта SNMP на коммутаторе. Агент будет прослушивать пакеты SNMP request на сервисном UDP-порту настроенного номера.

Пример

В данном примере показано, как настроить номер UDP-порта SNMP.

```
Switch#configure terminal
Switch(config)#snmp-server service-port 50000
Switch(config)#
```

57.12 snmp-server response broadcast-request

Данная команда позволяет разрешить серверу отвечать на широковещательные пакеты SNMP GetRequest. Чтобы запретить серверу отвечать на широковещательные пакеты SNMP GetRequest, воспользуйтесь формой **no** этой команды.

snmp-server response broadcast-request

no snmp-server response broadcast-request

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы разрешить серверу отвечать на широковещательные пакеты SNMP GetRequest, которые будут отправлены средствами NMS для определения сетевого устройства. Для применения данной функции необходимо включить ответ на широковещательные пакеты GetRequest.

Пример

В данном примере показано, как разрешить серверу отвечать на широковещательные пакеты SNMP GetRequest.

```
Switch#configure terminal
Switch(config)#snmp-server response broadcast-request
Switch(config)#
```

57.13 snmp trap link-status

Данная команда используется для включения отправки уведомлений об обнаружении/разрыве соединения (link-up / link-down), произошедшем на интерфейсе. Чтобы отключить отправку, воспользуйтесь формой **no** этой команды.

snmp trap link-status
no snmp trap link-status

Параметры

Нет.

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда используется для включения или отключения отправки SNMP trap об обнаружении/разрыве соединения (link-up / link-down) на интерфейсе.

Пример

В данном примере показано, как отключить отправку SNMP trap об обнаружении/разрыве соединения (link-up / link-down) на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#no snmp trap link-status
Switch(config-if)#
```

57.14 show snmp

Данная команда используется для отображения настроек SNMP.

show snmp {community | host | view | group | engineID}

Параметры

community	Укажите, чтобы отобразить информацию об SNMP-сообществе.
host	Укажите, чтобы отобразить информацию о получателе SNMP trap.
view	Укажите, чтобы отобразить информацию об SNMP View.
group	Укажите, чтобы отобразить информацию об SNMP-группе.
engineID	Укажите, чтобы отобразить информацию об SNMP local engine ID.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду для отображения информации об SNMP. При отображении строк SNMP community string созданные SNMPv1 или SNMPv2c-пользователи не будут отображены.

Пример

В примере ниже показано, как отобразить информацию об SNMP-сообществе.

```
Switch#show snmp community

Community : public
 Access : read-only
 View : CommunityView

Community : private
 Access : read-write
 View : CommunityView

Total Entries: 2

Switch#
```

В примере ниже показано, как отобразить настройки SNMP-сервера.

```
Switch# show snmp host

Host IP Address  : 10.20.30.40
SNMP Version     : V1
Community Name   : public
UDP Port         : 50001

Host IP Address  : 10.10.10.1
SNMP Version     : V3 noauthnopriv
SNMPv3 User Name : user1
UDP Port         : 50001

Host IPv6 Address: 1:12:123::100
SNMP Version     : V3 noauthnopriv
SNMPv3 User Name : user2
UDP Port         : 162

Total Entries: 3

Switch#
```

В примере ниже показано, как отобразить настройки MIB view.

```
Switch#show snmp view

View Name                Subtree              View Type
-------------------------------------------------------------
restricted               1.3.6.1.2.1.1                included
restricted               1.3.6.1.2.1.11               included
restricted               1.3.6.1.6.3.10.2.1           included
restricted               1.3.6.1.6.3.11.2.1           included
restricted               1.3.6.1.6.3.15.1.1           included
CommunityView            1                            included
CommunityView            1.3.6.1.6.3                  excluded
CommunityView            1.3.6.1.6.3.1                included

Total Entries: 8

Switch#
```

В примере ниже показано, как отобразить настройки SNMP-группы.

```
Switch# show snmp group

GroupName: public                           SecurityModel: v1
  ReadView     : CommunityView              WriteView    :
  NotifyView   : CommunityView
IP access control list:

GroupName: public                           SecurityModel: v2c
  ReadView     : CommunityView              WriteView    :
  NotifyView   : CommunityView
IP access control list:

GroupName: initial                          SecurityModel: v3/noauth
  ReadView     : restricted                 WriteView    :
  NotifyView   : restricted
IP access control list:

GroupName: private                          SecurityModel: v1
  ReadView     : CommunityView              WriteView    : CommunityView
  NotifyView   : CommunityView
IP access control list:

GroupName: private                          SecurityModel: v2c
  ReadView     : CommunityView              WriteView    : CommunityView
  NotifyView   : CommunityView
IP access control list:

Total Entries: 5

Switch#
```

В примере ниже показано, как отобразить SNMP engine ID.

```
Switch# show snmp engineID

Local SNMP engineID: 800000ab033c1e04a1b9e000

Switch#
```

57.15 show snmp user

Данная команда используется для отображения информации о настроенном SNMP-пользователе.

show snmp user [*USER-NAME***]**

Параметры

USER-NAME	(Опционально.) Укажите имя SNMP-пользователя, о котором необходимо отобразить информацию.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если имя пользователя не указано, будут отображены все настроенные пользователи. С помощью данной команды нельзя отобразить созданную строку community string.

Пример

В данном примере показано, как отобразить SNMP-пользователей.

```
Switch# show snmp user authuser

User name: authuser
  Security Model: v2c
  Group Name: VacmGroupName
IP access control list: HB5

User name: authuser
  Security Model: v3 priv
  Group Name: VacmGroupName
  Authentication Protocol: MD5
  Privacy Protocol: DES
  Engine ID: 0000009020000000C025808
IP access control list:

Total Entries: 2

Switch#
```

57.16 snmp-server community

Данная команда используется, чтобы настроить строку сообщества (community string) для доступа к SNMP. Для удаления строки community string воспользуйтесь формой **no** этой команды.

snmp-server community *COMMUNITY-STRING* **[view** *VIEW-NAME***] [ro | rw] [access** *IP-ACL-NAME***]**

no snmp-server community *COMMUNITY-STRING*

Параметры

COMMUNITY-STRING	Укажите строку community string. Максимальное количество символов в строке – 32.
view *VIEW-NAME*	(Опционально.) Укажите имя ранее настроенного view, которое доступно указанному SNMP-сообществу.
ro	(Опционально.) Укажите право «только чтение».
rw	(Опционально.) Укажите право «чтение/запись».
access *IP-ACL-NAME*	(Опционально.) Укажите имя стандартного списка доступа, дающего возможность пользователю использовать указанную строку community string при доступе к агенту SNMP. Укажите доступного пользователя в поле адреса источника записи списка доступа.

По умолчанию

Community	View Name	Access right
private	CommunityView	Read/Write (чтение/запись)
public	CommunityView	Read Only (только чтение)

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда предоставляет простой способ для создания строки community string для управления SNMPv1 и SNMPv2c. При настройке сообщества с помощью команды **snmp-server community** будут созданы две записи SNMP-группы: одна для SNMPv1 и другая для SNMPv2c, у которых имя сообщества совпадают с именами групп. Если **view** не указан, разрешен доступ ко всем объектам.

Пример

В данном примере показано, как создать MIB view «interfacesMibView» и строку community string «comaccess», с помощью которой можно получить право «чтение/запись» к созданному view «interfacesMibView».

```
Switch#configure terminal
Switch(config)#snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)#snmp-server community comaccess view interfacesMibView rw
Switch(config)#
```

57.17 snmp-server engineID local

Данная команда используется для указания SNMP engine ID на локальном устройстве. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

snmp-server engineID local *ENGINEID-STRING*
no snmp-server engineID local

Параметры

ENGINEID-STRING	Укажите строку engine ID. Максимальное количество символов в строке – 24.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

SNMP engine ID, уникальная строка для идентификации устройства, не отображается и не хранится в текущей конфигурации. По умолчанию строка генерируется автоматически. Строка, количество символов в которой менее 24, будет дополнена нулями, так чтобы общее количество символов составило 24.

Пример

В данном примере показано, как настроить SNMP engine ID со значением 332200000000000000000000.

```
Switch# configure terminal
Switch(config)# snmp-server engineID local 332200000000000000000000
Switch(config)#
```

57.18 snmp-server group

Данная команда используется для настройки SNMP-группы. Чтобы удалить SNMP-группу или удалить группу из используемой указанной модели безопасности, воспользуйтесь формой **no** этой команды.

snmp-server group *GROUP-NAME* **{v1 | v2c | v3 {auth | noauth | priv}} [read** *READ-VIEW***] [write** *WRITE-VIEW***] [notify** *NOTIFY-VIEW***] [access** *IP-ACL-NAME***]**
no snmp-server group *GROUP-NAME* **{v1 | v2c | v3 {auth | noauth | priv}}**

Параметры

GROUP-NAME	Укажите имя группы. Максимальное количество символов в строке – 32. Пробелы в строке недопустимы.
v1	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv1.
v2c	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv2c.
v3	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv3.
auth	Укажите для аутентификации пакетов. Данный параметр не используется для шифрования пакетов.
noauth	Укажите для отмены аутентификации и шифрования пакетов.
priv	Укажите для аутентификации и шифрования пакетов.
read *READ-VIEW*	(Опционально.) Укажите, чтобы обеспечить доступ к чтению пользователю данной группы.
write *WRITE-VIEW*	(Опционально.) Укажите, чтобы обеспечить доступ к записи пользователю данной группы.
notify *NOTIFY-VIEW*	(Опционально.) Укажите, чтобы обеспечить доступ для уведомлений пользователю данной группы. В данном уведомлении описывается объект, о состоянии которого пользователь данной группы узнает с помощью SNMP trap.
access *IP-ACL-NAME*	(Опционально.) Укажите стандартный IP-адрес списка управления доступом (ACL) для ассоциирования с группой.

По умолчанию

Group Name	Version	Security Level	Read View Name	Write View Name	Notify View
Initial	SNMPv3	noauth	Restricted	None	Restricted
Public	SNMPv1	None	CommunityView	None	CommunityView
Public	SNMPv2c	None	CommunityView	None	CommunityView
Private	SNMPv1	None	CommunityView	CommunityView	CommunityView
Private	SNMPv2c	None	CommunityView	CommunityView	CommunityView

По умолчанию нет списка управления доступом (ACL), ассоциированного с какой-либо SNMP-группой.

Режим ввода команды

Global Configuration Mode.

Использование команды

Для определения пользователя SNMP-группы необходимо указать разрешенную модель безопасности и право с помощью параметров *READ-VIEW*, *WRITE-VIEW* и *NOTIFY-VIEW*. Модель безопасности позволяет пользователю применять указанную версию SNMP при доступе к агенту SNMP.

Возможно создание групп с одинаковыми именами при указании разных моделей безопасности SNMPv1, SNMPv2c и SNMPv3 одновременно. При указании SNMPv3 доступно использование двух параметров **auth** и **priv** одновременно.

Чтобы загрузить новый профиль view для группы для определенной модели безопасности, удалите ранее созданную группу и создайте новую группу с новым профилем view.

Параметр *READ-VIEW* определяет MIB-объекты, которые доступны для чтения пользователю группы. Если *READ-VIEW* не указан, может быть прочитано Internet OID-пространство 1.3.6.1.

Параметр *WRITE-VIEW* определяет MIB-объекты, которые доступны для записи пользователю группы. Если *WRITE-VIEW* не указан, никакой из MIB-объектов не может быть записан.

Параметр *NOTIFY-VIEW* определяет MIB-объекты, с помощью которых система может сообщать о своем статусе в notify-пакетах уведомлений trap-менеджерам, которые идентифицированы указанным пользователем группы, выступающим в качестве строки Community String. Если *NOTIFY-VIEW* не указан, информация о MIB-объектах не будет получена.

Пример

В данном примере показано, как создать группу SNMP-сервера для доступа по SNMPv3 и SNMPv2c. Настроенная группа – guestgroup.

```
Switch#configure terminal
Switch(config)#snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)#snmp-server group guestgroup v3 auth read interfacesMibView
Switch(config)#snmp-server group guestgroup v2c read CommunityView write CommunityView
Switch(config)#
```

57.19 snmp-server host

Данная команда используется для указания получателя SNMP-уведомлений. Чтобы удалить получателя, воспользуйтесь формой **no** этой команды.

snmp-server host {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [version {1 | 2c | 3 {auth | noauth | priv}}]** *COMMUNITY-STRING* **[port** *PORT-NUMBER***]**

no snmp-server host {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [***COMMUNITY-STRING***]**

Параметры

IP-ADDRESS	Укажите IPv4-адрес узла-получателя сервера для SNMP-уведомлений.
IPV6-ADDRESS	Укажите IPv6-адрес узла-получателя сервера для SNMP-уведомлений.

version	(Опционально.) Укажите версию SNMP, которую необходимо использовать для отправки SNMP trap. Если версия не указана, по умолчанию используется SNMPv1. **1** – SNMPv1. **2c** – SNMPv2c. **3** – SNMPv3.
auth	(Опционально.) Укажите для аутентификации пакетов. Данный параметр не используется для шифрования пакетов.
noauth	(Опционально.) Укажите для отмены аутентификации и шифрования пакетов.
priv	(Опционально.) Укажите для аутентификации и шифрования пакетов.
COMMUNITY-STRING	Введите строку community string, которую необходимо отправить с notify-пакетами уведомлений. При указании версии 3 строка community string используется в качестве имени пользователя, как показано в примере команды **snmp-sever user**.
PORT-NUMBER	(Опционально.) Укажите номер UDP-порта. Номер UDP-порта trap по умолчанию – 162. Диапазон номеров UDP-порта: от 1 до 65535. Некоторые номера портов могут конфликтовать с другими протоколами.

По умолчанию

По умолчанию используется версия 1.

Режим ввода команды

Global Configuration Mode.

Использование команды

SNMP-уведомления отправляются в виде SNMP trap. Для отправки SNMP-уведомлений необходимо создать по крайней мере одного получателя при помощи команды **snmp-server host**. Для созданного пользователя укажите версию SNMP trap-пакетов. При указании SNMPv1 и SNMPv2c уведомления SNMP trap будут отправлены в PDU (Trap Protocol Data Unit). При указании SNMPv3 уведомления SNMP trap будут отправлены в SNMPv2-TRAP-PDU с заголовком SNMPv3.

При указании SNMPv1 или SNMPv2c для отправки SNMP trap на определенный узел указанная строка community string выступает в качестве строки SNMP trap.

При указании SNMPv3 для отправки SNMP trap на определенный узел укажите, необходима ли аутентификация и шифрование отправленных пакетов. Указанная строка community string выступает в качестве имени пользователя в пакетах SNMPv3. При использовании команды **snmp-server user** или **snmp-server user v3** сначала необходимо создать пользователя.

При отправке SNMP trap система проверит уведомления view, ассоциированные с указанным пользователем или именем сообщества. Если вариабельные привязки (binding variables), которые

должны быть отправлены с SNMP trap, отсутствуют в уведомлениях view, уведомления не будут отправлены на данный сервер.

Пример

В данном примере показано, как настроить SNMP trap-получателя с указанием версии 1 и со строкой community string «comaccess». SNMP trap-получатель – 163.10.50.126.

```
Switch#configure terminal
Switch(config)#snmp-server community comaccess rw
Switch(config)#snmp-server host 163.10.50.126 version 1 comaccess
Switch(config)#
```

В примере ниже показано, как настроить SNMP trap-получателя с указанием типа уровня безопасности аутентификации версии 3 и имени пользователя «useraccess». SNMP trap-получатель – 163.10.50.126.

```
Switch#configure terminal
Switch(config)#snmp-server group groupaccess v3 auth read CommunityView write CommunityView
Switch(config)#snmp-server user useraccess groupaccess v3 auth md5 12345678
Switch(config)#snmp-server host 163.10.50.126 version 3 auth useraccess
Switch(config)#
```

В следующем примере показано, как настроить SNMP trap-получателя с указанием версии 1 и со строкой community string «comaccess». SNMP trap-получатель – 163.10.50.126. Номер UDP-порта – 50001.

```
Switch#configure terminal
Switch(config)#snmp-server community comaccess rw
Switch(config)#snmp-server host 163.10.50.126 version 1 comaccess port 50001
Switch(config)#
```

57.20 snmp-server user

Данная команда используется для создания SNMP-пользователя. Чтобы удалить SNMP-пользователя, воспользуйтесь формой **no** этой команды.

snmp-server user *USER-NAME GROUP-NAME* **[encrypted] [auth {md5 | sha}** *AUTH-PASSWORD* **[priv** *PRIV-PASSWORD*]] **[access** *IP-ACL-NAME*]

no snmp-server user *USER-NAME GROUP-NAME*

Параметры

USER-NAME	Укажите имя пользователя. Максимальное количество символов в строке – 32. Пробелы в строке недопустимы.
GROUP-NAME	Укажите имя группы, к которой принадлежит данный пользователь. Пробелы в строке недопустимы.
encrypted	(Опционально.) Укажите для шифрования пароля.
auth	(Опционально.) Укажите тип аутентификации.

md5	(Опционально.) Укажите использование аутентификации HMAC-MD5-96.
sha	(Опционально.) Укажите использование аутентификации HMAC-SHA-96.
AUTH-PASSWORD	(Опционально.) Укажите пароль аутентификации в форме обычного текста. Для MD5 пароль может содержать от 8 до 16 символов, для SHA – от 8 до 20. При указании параметра **encrypted** длина пароля для MD5 составляет 32, для SHA – 40. В данном параметре используются шестнадцатеричные значения.
priv	(Опционально.) Укажите тип шифрования.
PRIV-PASSWORD	(Опционально.) Укажите пароль Private в форме обычного текста. Максимально допустимое количество символов – 16. При указании параметра **encrypted** фиксированная длина пароля – 32 символа.
access *IP-ACL-NAME*	(Опционально.) Укажите стандартный IP-адрес ACL для ассоциирования с пользователем.

По умолчанию

По умолчанию настроен один пользователь.
Имя пользователя – initial.
Имя группы – initial.

Режим ввода команды

Global Configuration Mode.

Использование команды

Для создания SNMP-пользователя укажите модель безопасности, которая будет использована данным пользователем, и группу, для которой создан данный пользователь. Для создания SNMPv3-пользователя необходимо указать пароль для аутентификации и шифрования.

Невозможно удалить SNMP-пользователя, который был ассоциирован с SNMP-сервером.

Пример

В данном примере показано, как настроить пароль в форме обычного текста для пользователя «user1» в группе «public» в версии SNMPv3.

```
Switch#configure terminal
Switch(config)# snmp-server user user1 public v3 auth md5 authpassword priv privpassword
Switch(config)#
```

В примере ниже показано, как использовать строку MD5 digest вместо пароля в форме обычного текста.

```
Switch#configure terminal
Switch(config)# snmp-server user user1 public v3 encrypted auth md5
00112233445566778899AABBCCDDEEFF
Switch(config)#
```

57.21 snmp-server view

Данная команда используется для создания или изменения записи view. Чтобы удалить указанную запись SNMP view, воспользуйтесь формой **no** этой команды.

snmp-server view *VIEW-NAME OID-TREE* **{included | excluded}**
no snmp-server view *VIEW-NAME*

Параметры

VIEW-NAME	Укажите имя записи view. Диапазон значений: от 1 до 32 символов. Пробелы в строке недопустимы.
OID-TREE	Укажите идентификатор объекта (Object IDentifier, OID) под-дерева ASN.1, который необходимо включить или исключить из View. Для идентификации под-дерева введите строку, состоящую либо из чисел, например, 1.3.6.2.4, либо из слов, например, system. При указании семейства под-деревьев используйте подстановочный знак (*) перед каждым идентификатором под-дерева.
included	Укажите под-дерево, которое необходимо включить в SNMP View.
excluded	Укажите под-дерево, которое необходимо исключить из SNMP View.

По умолчанию

VIEW-NAME	OID-TREE	View Type
Restricted	1.3.6.1.2.1.1	Included
Restricted	1.3.6.1.2.1.11	Included
Restricted	1.3.6.1.6.3.10.2.1	Included
Restricted	1.3.6.1.6.3.11.2.1	Included
Restricted	1.3.6.1.6.3.15.1.1	Included
CommunityView	1	Included
CommunityView	1.3.6.1.6.3	Excluded
CommunityView	1.3.6.1.6.3.1	Included

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы создать view MIB-объектов.

Пример

В данном примере показано, как создать MIB view и предоставить доступ для чтения SNMP-группе, ассоциированной с данным MIB view. Настроенный MIB view – interfacesMibView. SNMP-группа – guestgroup.

```
Switch#configure terminal
Switch(config)#snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)#snmp-server group guestgroup v3 auth read interfacesMibView
Switch(config)#
```

58. Команды Spanning Tree Protocol (STP)

58.1 clear spanning-tree detected-protocols

Данная команда используется для перезапуска процесса миграции протокола.

clear spanning-tree detected-protocols {all | interface *INTERFACE-ID***}**

Параметры

all	Укажите, чтобы запустить действие обнаружения для всех портов.
interface *INTERFACE-ID*	Укажите интерфейс порта, на котором необходимо запустить действие обнаружения.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

С помощью данной команды во время миграции протокола порт будет переведен в состояние *SEND_RSTP*. Данное действие можно использовать, чтобы проверить, все ли устаревшие мосты на LAN были удалены. При отсутствии моста STP на данной LAN порт будет работать в выбранном режиме RSTP или MSTP. В противном случае порт будет работать в режиме STP.

Пример

В данном примере показано, как запустить процесс миграции протокола для всех портов.

```
Switch#clear spanning-tree detected-protocols all

Clear spanning-tree detected-protocols? (y/n) [n] y

Switch#
```

58.2 show spanning-tree

Данная команда используется для отображения информации о работе протокола Spanning Tree и применяется только для STP и RSTP.

show spanning-tree [interface [_INTERFACE-ID_ **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите ID интерфейса для отображения.

,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду для отображения настроек Spanning Tree одного связующего дерева в режиме, совместимом с RSTP или STP.

Пример

В данном примере показано, как отобразить информацию о Spanning Tree при включенном STP.

```
Switch#show spanning-tree

 Spanning Tree: Enabled
 Protocol Mode: RSTP
 Tx-hold-count: 6
 Root ID Priority: 32768
         Address: 3C-1E-04-A1-B9-E0
         Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
 Bridge  ID Priority: 32768 (priority 32768  sys-id-ext 0)
         Address: 3C-1E-04-A1-B9-E0
         Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec,
 Topology Changes Count: 0

                                          Priority Link
 Interface      Role       State      Cost      .Port#   Type   Edge
 ---------      ----       -----      ----      -------  -----  ----
 eth1/0/3       designated forwarding 20000     128.3    p2p    non-edge
 eth1/0/5       backup     blocking   200000    128.5    p2p    non-edge
 eth1/0/6       backup     blocking   200000    128.6    shared non-edge
 eth1/0/7       root       forwarding 2000      128.7    P2p    non-edge

Switch#
```

58.3 show spanning-tree configuration interface

Данная команда используется для отображения информации о настройках интерфейса STP.

show spanning-tree configuration interface [*INTERFACE-ID* **[, | -]]**

Параметры

INTERFACE-ID	(Опционально.) Укажите ID интерфейса для отображения.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы отобразить настройки интерфейса Spanning Tree. Команда может применяться для всех версий STP.

Пример

В данном примере показано, как отобразить информацию о настройках Spanning Tree для интерфейса Ethernet 1/0/1.

```
Switch# show spanning-tree configuration interface eth1/0/1

eth1/0/1
 Spanning tree state : Enabled
 Port path cost: 0
 Port priority: 128
 Port Identifier:  128.1
 Link type: auto
 Port fast: auto
 Guard root: Disabled
 TCN filter : Disabled
 Bpdu forward: Disabled

Switch#
```

58.4 snmp-server enable traps stp

Данная команда позволяет включить отправку SNMP-уведомлений для STP. Чтобы отключить отправку уведомлений для STP, воспользуйтесь формой **no** этой команды.

snmp-server enable traps stp [new-root] [topology-chg]

no snmp-server enable traps stp [new-root] [topology-chg]

Параметры

new-root	(Опционально.) Укажите для отправки уведомлений о новом корне STP.
topology-chg	(Опционально.) Укажите для отправки уведомлений об изменении STP-топологии.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы включить/отключить отправку trap-уведомлений. Если ни один из опциональных параметров не указан, будут отключены оба типа уведомлений STP.

Пример

В данном примере показано, как включить отправку всех STP trap на узел 10.9.18.100, используя строку сообщества «public».

```
Switch#configure terminal
Switch(config)#snmp-server enable traps
Switch(config)#snmp-server enable traps stp
Switch(config)#snmp-server host 10.9.18.100 version 2c public
Switch(config)#
```

58.5 spanning-tree global state

Данная команда используется для включения/отключения глобального состояния STP. Чтобы отключить глобальное состояние STP, воспользуйтесь формой **no** этой команды.

spanning-tree global state {enable | disable}

no spanning-tree global state

Параметры

enable	Укажите, чтобы включить глобальное состояние STP.
disable	Укажите, чтобы отключить глобальное состояние STP.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы включить/отключить функцию Spanning Tree глобально.

Пример

В данном примере показано, как включить функцию Spanning Tree.

```
Switch#configure terminal
Switch(config)#spanning-tree global state enable
Switch(config)#
```

58.6 spanning-tree (timers)

Данная команда используется для настройки значений таймеров Spanning Tree. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

spanning-tree {hello-time *SECONDS* **| forward-time** *SECONDS* **| max-age** *SECONDS***}**
no spanning-tree {hello-time | forward-time | max-age}

Параметры

hello-time *SECONDS*	Укажите интервал между циклической передачей конфигурационных сообщений. Диапазон значений: от 1 до 2 секунд.
forward-time *SECONDS*	Укажите время задержки продвижения (Forward Delay), используемое STP для перехода из состояния listening и learning в состояние forwarding. Диапазон значений: от 4 до 30 секунд.
max-age *SECONDS*	Укажите максимальное время жизни сообщения BDPU. Диапазон значений: от 6 до 40 секунд.

По умолчанию

Значение параметра **hello-time** по умолчанию – 2 секунды.
Значение параметра **forward-time** по умолчанию – 15 секунд.
Значение параметра **max-age** по умолчанию – 20 секунд.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить значения таймеров Spanning Tree.

Пример

В данном примере показано, как настроить значения таймеров Spanning Tree.

```
Switch#configure terminal
Switch(config)#spanning-tree hello-time 1
Switch(config)#spanning-tree forward-time 16
Switch(config)#spanning-tree max-age 21
Switch(config)#
```

58.7 spanning-tree state

Данная команда используется для включения/отключения STP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

spanning-tree state {enable | disable}
no spanning-tree state

Параметры

enable	Укажите, чтобы включить STP для настраиваемого интерфейса.
disable	Укажите, чтобы отключить STP для настраиваемого интерфейса.

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Если Spanning Tree включено, BPDU, полученный портом, будет либо отправлен, либо обработан. Используя данную команду, не допускайте появления петель. Данная команда не будет применена, если функция L2PT включена для STP.

Пример

В данном примере показано, как включить Spanning Tree на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#spanning-tree state enable
Switch(config-if)#
```

58.8 spanning-tree cost

Данная команда используется для настройки значения стоимости пути на указанном порту. Чтобы определить стоимость пути автоматически, воспользуйтесь формой **no** этой команды.

spanning-tree cost *COST*
no spanning-tree cost

Параметры

COST	Укажите стоимость пути для порта. Диапазон значений: от 1 до 200000000.

По умолчанию

По умолчанию стоимость пути определяется на основе настроек полосы пропускания интерфейса.

Режим ввода команды

Interface Configuration Mode.

Использование команды

В режимах, совместимых с STP и RSTP, для одного связующего дерева стоимость пути, заданная администратором, используется для достижения корня (root). В режиме MSTP региональным корнем CIST (CIST regional root) используется стоимость пути, заданная администратором, для достижения корня CIST (CIST root).

Пример

В данном примере показано, как настроить значение стоимости пути на интерфейсе Ethernet 1/0/7. Указанное значение – 20000.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree cost 20000
Switch(config-if)#
```

58.9 spanning-tree guard root

Данная команда используется для включения функции STP Root Guard. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

spanning-tree guard root
no spanning-tree guard root

Параметры

Нет.

По умолчанию

По умолчанию функция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

BPDU Guard предотвращает превращение порта в корневой порт и ограничивает доступ внешним мостам, находящимся не под полным контролем администратора, к основному региону сети активной топологии связующего дерева.

Порт, которому было отказано в присвоении роли корневого порта (root port), сможет работать только в качестве назначенного порта (designated port). При получении конфигурационного BPDU с более высоким приоритетом порт начнет работать в качестве альтернативного порта (alternate port) в состоянии blocking. Получение BPDU с более высоким приоритетом не повлияет на построение STP. Порт будет прослушивать сообщения BPDU. Если время ожидания получения BPDU с наибольшим

приоритетом истечет, порт начнет работать в качестве назначенного порта.

Когда функция Guard Root сработает и порт начнет работать в качестве альтернативного порта, будет сгенерировано системное сообщение. Данные настройки действительны для всех версий Spanning Tree.

Пример

В данном примере показано, как предотвратить смену роли порта на роль корневого порта (root port) для интерфейса Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#spanning-tree guard root
Switch(config-if)#
```

58.10 spanning-tree link-type

Данная команда используется, чтобы настроить тип соединения (link type) для порта. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

spanning-tree link-type {point-to-point | shared}

no spanning-tree link-type

Параметры

point-to-point	Укажите тип соединения «точка-точка» (point-to-point, P2P).
shared	Укажите тип соединения для подключения к сети общего пользования (shared media).

По умолчанию

Если параметры не указаны, тип соединения по умолчанию назначается на основе настроек дуплекса.

Режим ввода команды

Interface Configuration Mode.

Использование команды

На портах, функционирующих в режиме полного дуплекса, устанавливается соединение типа «точка-точка»; порты, работающие в режиме полудуплекса, считаются портами общего пользования (shared port). Так как быстрый переход в состояние forwarding при использовании типа соединения shared media невозможен, рекомендуется использовать автоматическое определение типа соединения модулем STP.

Данные настройки доступны для всех режимов Spanning Tree.

Пример

В данном примере показано, как настроить тип соединения «точка-точка» для интерфейса Ethernet 1/0/7.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree link-type point-to-point
Switch(config-if)#
```

58.11 spanning-tree mode

Данная команда используется для настройки режима STP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

spanning-tree mode {mstp | rstp |stp}
no spanning-tree mode

Параметры

mstp	Укажите Multiple Spanning Tree Protocol (MSTP).
rstp	Укажите Rapid Spanning Tree Protocol (RSTP).
stp	Укажите Spanning Tree Protocol (совместимый с IEEE 802.1D).

По умолчанию

Режим по умолчанию – RSTP.

Режим ввода команды

Global Configuration Mode.

Использование команды

Если настраивается режим STP или RSTP, все текущие MSTP-экземпляры будут отменены автоматически. При изменении режима Spanning Tree все порты перейдут в состояние отбрасывания (discarding).

Пример

В данном примере показано, как настроить текущую версию протокола STP на RSTP.

```
Switch#configure terminal
Switch(config)#spanning-tree mode rstp
Switch(config)#
```

58.12 spanning-tree portfast

Данная команда используется для настройки режима Port Fast Mode на порту. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

spanning-tree portfast {disable | edge| network}
no spanning-tree portfast

Параметры

disable	Укажите для включения режима Fast Disable Mode на порту.
edge	Укажите для включения режима Fast Edge Mode на порту.
network	Укажите для включения режима Fast Network Mode на порту.

По умолчанию

Параметр по умолчанию – **edge.**

Режим ввода команды

Interface Configuration Mode.

Использование команды

На порту может быть установлен один из трех режимов Port Fast Mode:

Edge Mode: при установлении соединения порт сразу же переходит в состояние forwarding, не дожидаясь задержки продвижения (Forward Delay). Рабочее состояние интерфейса, на котором BPDU было получено позже, будет изменено на состояние non-port-fast.

Disable Mode: порт всегда находится в состоянии non-port-fast и будет ждать, пока Forward Delay не перейдет в состояние forwarding.

Network Mode: порт находится в состоянии non-port-fast в течение трех секунд. Не получив BPDU, порт переходит в состояние port-fast, за которым следует состояние forwarding. Состояние порта, на котором BPDU было получено позже, будет изменено на состояние non-port-fast.

Применяя данную команду, не допускайте появления петель в топологии и петель во время передачи пакетов данных, которые нарушают работу сети.

Пример

В данном примере показано, как настроить режим Port Fast Edge Mode для интерфейса Ethernet- 1/0/7.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree portfast edge
Switch(config-if)#
```

58.13 spanning-tree port-priority

Данная команда используется для настройки значения приоритета STP на указанном порту. Команда применима только для версий RSTP и STP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

spanning-tree port-priority *PRIORITY*
no spanning-tree port-priority

Параметры

PRIORITY	Укажите приоритет порта в диапазоне от 0 до 240.

По умолчанию

Значение по умолчанию – 128.

Режим ввода команды

Interface Configuration Mode.

Использование команды

При присвоении роли порту используется его идентификатор, который состоит из приоритета и номера порта. Чем ниже число, тем выше приоритет. Данный параметр применим только в режимах RSTP или STP.

Пример

В данном примере показано, как настроить приоритет для интерфейса Ethernet 1/0/7 со значением 0.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree port-priority 0
Switch(config-if)#
```

58.14 spanning-tree priority

Данная команда используется для настройки приоритета моста. Команда применима только для версий RSTP и STP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

spanning-tree priority *PRIORITY*

no spanning-tree priority

Параметры

PRIORITY	Укажите Bridge-ID Spanning Tree, который состоит из приоритета и MAC-адреса моста. Bridge-ID является важным фактором в топологии Spanning Tree. Диапазон значений: от 0 до 61440.

По умолчанию

Значение по умолчанию – 32768.

Режим ввода команды

Global Configuration Mode.

Использование команды

Выбор корневого моста зависит от значение приоритета моста и системного MAC-адреса. Значение приоритета моста должно делиться на 4096. Чем меньше число, тем выше приоритет.

Данные настройки применимы для версий STP и RSTP протокола Spanning Tree. В режиме MSTP используйте команду **spanning-tree mst priority**, чтобы настроить приоритет для MSTP-экземпляра.

Пример

В данном примере показано, как настроить приоритет моста STP со значением 4096.

```
Switch#configure terminal
Switch(config)#spanning-tree priority 4096
Switch(config)#
```

58.15 spanning-tree tcnfilter

Данная команда используется для включения фильтрации уведомлений об изменении топологии сети TCN (Topology Change Notification) на указанном интерфейсе. Чтобы отключить фильтрацию TCN, воспользуйтесь формой **no** этой команды.

spanning-tree tcnfilter

no spanning-tree tcnfilter

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Фильтрация TCN используется для защиты ISP от подключения внешних мостов, находящихся не под полным контролем администратора, к основному региону сети, в котором в данной ситуации произойдет очистка (flush) адресов.

В режиме фильтрации уведомление TCN об изменении топологии, полученное на порту, игнорируется. Данные настройки действительны для всех режимов Spanning Tree.

Пример

В данном примере показано, как включить фильтрацию TCN на интерфейсе Ethernet 1/0/7.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree tcnfilter
Switch(config-if)#
```

58.16 spanning-tree tx-hold-count

Данная команда используется для ограничения максимального количества BPDU, которые могут быть отправлены перед паузой в одну секунду. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

spanning-tree tx-hold-count *VALUE*

no spanning-tree tx- hold-count

Параметры

VALUE	Укажите максимальное количество BPDU, которые могут быть отправлены перед паузой в одну секунду. Диапазон значений: от 1 до 10.

По умолчанию

Значение по умолчанию – 6.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы указать максимальное количество отправляемых BPDU. Передача BPDU на порт контролируется счетчиком, значение которого увеличивается при каждой отправке BPDU и уменьшается раз в секунду. Передача BPDU приостанавливается на одну секунду, если счетчик достигает значения параметра hold count.

Пример

В данном примере показано, как настроить параметр hold count со значением 5.

```
Switch#configure terminal
Switch(config)#spanning-tree tx-hold-count 5
Switch(config)#
```

58.17 spanning-tree forward-bpdu

Данная команда используется для включения BDPU Forwarding в Spanning Tree. Чтобы отключить BDPU Forwarding в Spanning Tree, воспользуйтесь формой **no** этой команды.

spanning-tree forward-bpdu
no spanning-tree forward-bpdu

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

При использовании данной команды полученные STP BPDU будут перенаправлены на все

member-порты VLAN без тега. Данная команда не будет применена, если функция L2PT включена для STP.

Пример

В данном примере показано, как включить BDPU Forwarding в Spanning Tree.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#spanning-tree forward-bpdu
Switch(config-if)#
```

59. Команды Storm Control

59.1 snmp-server enable traps storm-control

Данная команда используется, чтобы включить и настроить отправку SNMP-уведомлений для Storm Control. Для отключения отправки SNMP-уведомлений воспользуйтесь формой **no** этой команды.

snmp-server enable traps storm-control [storm-occur] [storm-clear]

no snmp-server enable traps storm-control [storm-occur] [storm-clear]

Параметры

storm-occur	(Опционально.) Укажите для отправки уведомлений при возникновении шторма.
storm-clear	(Опционально.) Укажите для отправки уведомлений при предотвращении шторма.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для включения/отключения отправки SNMP-уведомлений для Storm Control. Если параметры не указаны, включены/отключены оба типа уведомлений.

Пример

В данном примере показано, как включить отправку trap-сообщений при возникновении и предотвращении шторма.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps storm-control
Switch(config)#
```

59.2 storm-control

Данная команда используется для защиты устройства от штормовых атак широковещательных и многоадресных пакетов или пакетов с неизвестным адресом назначения. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

storm-control {{broadcast | multicast | unicast} level {pps *PPS-RISE* **[***PPS-LOW***] | kbps** *KBPS-RISE* **[***KBPS-LOW***] |** *LEVEL-RISE* **[***LEVEL-LOW***]} | action {shutdown | drop | none}}**

no storm-control {broadcast | multicast | unicast | action}

Параметры

broadcast	Укажите для ограничения скорости широковещательной рассылки.
multicast	Укажите для ограничения скорости многоадресной рассылки.
unicast	Укажите, чтобы в режиме **shutdown** применять команду как к известным, так и к неизвестным одноадресным пакетам. При достижении на порту установленного лимита пакетов порт будет отключен. Если указан другой режим, команда будет применена только к неизвестным одноадресным пакетам.
level pps *PPS-RISE* **[***PPS-LOW***]**	Укажите пороговое значение пакетов в секунду. Диапазон значений: от 0 до 2147483647. Если минимальный уровень (Low Level) PPS не указан, значение по умолчанию составляет 80% от указанного максимального (Rise) PPS.
level kbps *KBPS-RISE* **[***KBPS-LOW***]**	Укажите пороговое значение скорости передачи трафика, полученного на порту, в битах в секунду**.** Диапазон значений: от 0 до 2147483647. Если минимальный уровень (Low Level) KBPS не указан, значение по умолчанию составляет 80% от указанного максимального (Rise) KBPS.
level *LEVEL-RISE* **[***LEVEL-LOW***]**	Укажите пороговое значение трафика, полученного на порту, в процентах от общей пропускной способности. Диапазон значений: от 0 до 100. Если минимальный уровень (Low Level) не указан, значение по умолчанию составляет 80% от указанного максимального уровня (Rise Level).
action shutdown	Укажите, чтобы отключить порт при достижении указанного максимального порогового значения.
action drop	Укажите, чтобы отбросить пакеты, которые превышают максимальный порог.
action none	Укажите, чтобы не фильтровать Storm пакеты.

По умолчанию

По умолчанию функция Storm Control для защиты от атак широковещательных, многоадресных и одноадресных (DLF) пакетов отключена.
При возникновении шторма действие по умолчанию – drop.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Функция Storm Control используется для защиты сети от штормовых атак широковещательных и многоадресных пакетов или пакетов с неизвестным адресом назначения лавинной рассылки. Используйте команду **storm-control**, чтобы включить Storm Control для определенного типа трафика на интерфейсе.

Восстановить порт при возникновении ошибки можно двумя способами.

Пользователь может использовать команду **errdisable recovery cause**, чтобы включить автоматическое восстановление портов, которые были отключены по ошибке Storm Control.

Пользователь может вручную восстановить порт, введя команду **shutdown**, а затем команду **no shutdown** для порта.

Существует только один режим (в процентах, кбит/с или PPS), который может быть применен на интерфейсе. На интерфейсе, если указанный позже параметр режима отличается от предыдущего режима, предыдущие настроенные штормы будут сброшены до состояния по умолчанию (отключены в этой спецификации).

Из-за аппаратных ограничений, когда режим установлен в процентах или кбит/с:

Действие не может быть задано для режима Shutdown (отключение).

Для режимов Drop (отбрасывание), None (без действия) отсутствуют трапы и журналы.

Эта функция не может дать точный уровень подавления общей полосы пропускания в процентах (от 0 до 100) для определенного физического интерфейса. Текущая формула расчета предполагает, что размер пакета составляет 64 байта.

Пример

В данном примере показано, как включить Storm Control для управления широковещательным штормом на интерфейсах Ethernet 1/0/1 и Ethernet 1/0/2. На Ethernet 1/0/1 установлен порог до 500 пакетов в секунду с действием отключения (shutdown). На интерфейсе порта 2 установлен максимальный порог 70% с минимальным уровнем (Low Level) 60% и действием отбрасывания (drop).

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#storm-control broadcast level pps 500
Switch(config-if)#storm-control action shutdown
Switch(config-if)#exit
Switch(config)#interface eth1/0/2
Switch(config-if)#storm-control broadcast level 70 60
Switch(config-if)#storm-control action drop
Switch(config-if)#
```

59.3 storm-control polling

Данная команда используется для настройки интервала опроса (Polling Interval) для подсчета количества полученных пакетов. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

storm-control polling {interval *SECONDS* **| retries {***NUMBER* **| infinite}}**

no storm-control polling {interval | retries}

Параметры

interval *SECONDS*	Укажите интервал опроса для подсчета количества полученных пакетов. Диапазон значений: от 5 до 600 секунд.

retries *NUMBER*	Укажите количество попыток интервалов между запросами. Если в режиме **shutdown** шторм продолжается во время установленных значений попыток, порт перейдет в состояние Error-Disabled. Диапазон значений: от 0 до 360. 0 означает, что при обнаружении шторма порт в режиме **shutdown** сразу же будет отключен из-за ошибки. **Infinite** означает, что порт в режиме **shutdown** не будет отключен из-за ошибки даже при обнаружении шторма.

По умолчанию

Интервал опроса по умолчанию – 5 секунд.
Количество попыток по умолчанию – 3.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы указать интервал выборки для подсчета количества полученных пакетов.

Пример

В данном примере показано, как указать интервал опроса со значением 15 секунд.

```
Switch#configure terminal
Switch(config)#storm-control polling interval 15
Switch(config)#
```

59.4 show storm-control

Данная команда используется для отображения текущих настроек функции Storm Control.

show storm-control interface *INTERFACE-ID* **[, | -] [broadcast | multicast | unicast]**

Параметры

INTERFACE-ID	Укажите ID интерфейса порта.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
broadcast	(Опционально.) Укажите, чтобы отобразить текущие настройки шторма широковещательных пакетов (Broadcast Storm).
multicast	(Опционально.) Укажите, чтобы отобразить текущие настройки шторма многоадресных пакетов (Multicast Storm).

unicast	(Опционально.) Укажите, чтобы отобразить текущие настройки шторма одноадресных пакетов (DLF).

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если тип пакета не указан, будут отображены настройки всех типов Storm Control.

Пример

В данном примере показано, как отобразить текущие настройки Storm Control для широковещательных пакетов в диапазоне интерфейсов Ethernet 1/0/1-1/0/6.

```
Switch#show storm-control interface ethe1/0/1-6 broadcast

 Interface   Action   Threshold            Current      State
 ------------------------------------------------------------------
 eth1/0/1    Drop     500/300 pps          200 pps      Forwarding
 eth1/0/2    Drop     80/64 %              20 %         Forwarding
 eth1/0/3    Drop     80/64 %              80 %         Dropped
 eth1/0/4    Shutdown 600/400 pps          300 pps      Forwarding
 eth1/0/5    None     60000/50000 kbps     2000 kbps    Forwarding
 eth1/0/6    None     -                    -            Inactive

 Total Entries: 6

Switch#
```

В примере ниже показано, как отобразить все настройки Storm Control для диапазона интерфейсов Ethernet 1/0/1-1/0/2.

```
Switch#show storm-control interface eth1/0/1-2

Polling Interval       : 15 sec          Shutdown Retries       : Infinite
Trap                   : Disabled
Interface      Storm         Action      Threshold     Current    State
---------------------- ----------------------------------------------
eth1/0/1       Broadcast     Drop         80/64 %       50%        Forwarding
eth1/0/1       Multicast     Drop         80/64 %       50%        Forwarding
eth1/0/1       Unicast       Drop         80/64 %       50%        Forwarding
eth1/0/2       Broadcast     Shutdown     500/300 pps   -          Error Disabled
eth1/0/2       Multicast     Shutdown     500/300 pps   -          Error Disabled
eth1/0/2       Unicast       Shutdown     500/300 pps   -          Error Disabled

Total Entries: 6

Switch#
```

Отображаемые параметры

Interface	ID интерфейса.
Action	Настраиваемые действия. Возможны следующие действия: Drop (отбрасывание), Shutdown (отключение), None (без действия).
Threshold	Настраиваемое пороговое значение.
Current	Фактическая текущая скорость трафика, которая проходит через интерфейс, единицей которой могут быть проценты, кбит/с, PPS в зависимости от настроенного режима. Аппаратно скорость может быть подсчитана только в PPS, приблизительно равного значению в процентах и кбит/с.
State	Текущее состояние Storm Control на указанном интерфейсе для данного типа трафика. Возможны следующие состояния: **Forwarding:** шторма не обнаружено. **Dropped:** шторм обнаружен, и штормовой трафик, превышающий пороговое значение, отбрасывается. **Error Disabled:** порт отключен из-за шторма. **Link Down:** порт физически отключен. **Inactive:** Storm Control не включен для данного типа трафика.

60. Команды Surveillance VLAN

60.1 surveillance vlan

Данная команда используется для глобального включения функции Surveillance VLAN и ее настройки. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

surveillance vlan *VLAN-ID*
no surveillance vlan

Параметры

VLAN-ID	Укажите VLAN ID Surveillance VLAN в диапазоне от 2 до 4094.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду для глобального включения функции Surveillance VLAN и ее настройки на коммутаторе. На коммутаторе может быть настроена только одна Surveillance VLAN. Данная Surveillance VLAN поддерживает распознавание сетевых устройств для наблюдения, таких как IP-камеры (IPC) и сетевые видеорегистраторы (NVR), использующих протокол ONVIF.

Для включения функции Surveillance VLAN необходимо применить команду **surveillance vlan** в режиме Global Configuration Mode и команду **surveillance vlan enable** в режиме Interface Configuration Mode.

При включении на порту Surveillance VLAN порт будет автоматически распознан как нетегированный member-порт Surveillance VLAN, полученные нетегированные пакеты surveillance будут перенаправлены в Surveillance VLAN. При соответствии исходных MAC-адресов пакетов адресам уникального идентификатора организации (OUI), настроенным при помощи команды **surveillance vlan mac-address**, полученные пакеты распознаются как пакеты surveillance.

Auto-Surveillance VLAN можно использовать для передачи видеотрафика с IP-камеры и связанных с ней компонентов, таких как сервер для управления системой видеонаблюдения (VMS), клиент VMS и видеокодер. Эти устройства могут быть распознаны адресами уникального идентификатора организации (OUI) и протоколом ONVIF. Если IP-камера распознана протоколом ONVIF, коммутатор изучит ее на порту при помощи отслеживания пакетов Hello/ProbeMatch, а затем встроит порт в Surveillance VLAN.

Коммутатор рассматривает узел как сетевой видеорегистратор, как только он подключается к IP-камере через HTTP, HTTPS или RTSP. Коммутатор изучит видеорегистратор на порту и переместит его в Surveillance VLAN до тех пор, пока не истечет срок службы механизма устаревания или не будет удален кабель LAN.

Когда узел отправляет ARP-запрос на IP-камеру, коммутатор по-прежнему рассматривает данный узел как сетевой видеорегистратор, но временно перемещает его в Surveillance VLAN. Узел будет автоматически удален из Surveillance VLAN примерно через 30 секунд, если он больше не распознается как сетевой видеорегистратор.

Примечание: один и тот же ПК или ПК, подключенные к одному порту LAN на коммутаторе, не могут одновременно управлять коммутатором и подключенными к нему IP-камерами.

Если IP-камера распознается по OUI-адресу, коммутатор определит, является ли полученный пакет видеопакетом, проверив MAC-адрес IP-камеры. Если MAC-адреса источника нетегированных пакетов совпадают с MAC-адресом IP-камеры, то данные пакеты распознаются как видеопакеты и передаются в Surveillance VLAN. Если входящий видеопакет тегирован, а его VLAN ID совпадает с Surveillance VLAN ID, пакету будет присвоен приоритет видеотрафика.

Если IP-камера одновременно распознается и по OUI-адресу, и по ONVIF-протоколу, то данная IP-камера будет распознана по ONVIF-протоколу и включится. Если использовать ONVIF-протокол невозможно, IP-камера будет распознана по OUI-адресу.

VLAN необходимо создать перед ее назначением в качестве Surveillance VLAN.

Настроенную Surveillance VLAN нельзя удалить с помощью команды **no vlan**.

Пример

В данном примере показано, как включить функцию Surveillance VLAN и настроить VLAN 1001 в качестве Surveillance VLAN.

```
Switch#configure terminal
Switch(config)#surveillance vlan 1001
Switch(config)#
```

60.2 surveillance vlan aging

Данная команда используется для настройки времени устаревания (Aging Time) для устаревших динамических member-портов Surveillance VLAN. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

surveillance vlan aging *MINUTES*
no surveillance vlan aging

Параметры

MINUTES	Укажите время устаревания Surveillance VLAN в диапазоне от 1 до 65535 минут.

По умолчанию

Значение по умолчанию – 720 минут.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить время устаревания для устройства видеонаблюдения (Surveillance) и автоматически изученных member-портов Surveillance VLAN.

Когда последнее устройство Surveillance, подключенное к порту, перестает отправлять трафик и MAC-адрес данного устройства устаревает, запускается таймер времени устаревания Surveillance VLAN. По истечении данного времени порт будет удален из Surveillance VLAN.

Если трафик surveillance возобновляется в течение времени устаревания, таймер будет отменен.

Пример

В данном примере показано, как настроить время устаревания Surveillance VLAN. Указанное значение – 30 минут.

```
Switch#configure terminal
Switch(config)#surveillance vlan aging 30
Switch(config)#
```

60.3 surveillance vlan enable

Данная команда используется для включения функции Surveillance VLAN на портах. Чтобы отключить функцию Surveillance VLAN на портах, воспользуйтесь формой **no** этой команды.

surveillance vlan enable
no surveillance vlan enable

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и port-channel.

Команда применяется на портах доступа и гибридных портах.

Для включения функции Surveillance VLAN необходимо применить команду **surveillance vlan** в режиме Global Configuration Mode и команду **surveillance vlan enable** в режиме Interface Configuration Mode.

При включении на порту Surveillance VLAN порт будет автоматически распознан как нетегированный member-порт Surveillance VLAN. Полученные нетегированные пакеты surveillance будут перенаправлены в Surveillance VLAN. При соответствии исходных MAC-адресов пакетов адресам уникального идентификатора организации (OUI), настроенным при помощи команды **surveillance vlan mac-address**, полученные пакеты распознаются как пакеты surveillance.

Пример

В данном примере показано, как включить функцию Surveillance VLAN на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#surveillance vlan enable
Switch(config-if)#
```

60.4 surveillance vlan mac-address

Данная команда используется для добавления уникального идентификатора организации (OUI), определяемого с устройства системы видеонаблюдения в Surveillance VLAN. Чтобы удалить OUI устройства Surveillance, воспользуйтесь формой **no** этой команды.

surveillance vlan mac-address *MAC-ADDRESS MASK* **[component-type {vms | vms-client | video-encoder | network-storage | other} description** *TEXT***]**

no surveillance vlan mac-address *MAC-ADDRESS MASK*

Параметры

MAC-ADDRESS	Укажите MAC-адрес OUI.
MASK	Укажите соответствующую битовую маску MAC-адреса OUI.
component-type	(Опционально.) Укажите устройство системы видеонаблюдения, которое может быть автоматически обнаружено при помощи Surveillance VLAN.
vms	(Опционально.) Укажите сервер VMS (Video Management Server – сервер для управления системой видеонаблюдения).
vms-client	(Опционально.) Укажите клиента VMS в системе видеонаблюдения.
video-encoder	(Опционально.) Укажите видеокодер в системе видеонаблюдения.
network-storage	(Опционально.) Укажите сетевое хранилище в системе видеонаблюдения.
other	(Опционально.) Укажите другие устройства в системе видеонаблюдения (IP Surveillance Devices).
description *TEXT*	(Опционально.) Укажите описание OUI. Максимальное количество символов – 32.

По умолчанию

OUI Address	Mask	Component Type	Description
28-10-7B-00-00-00	FF-FF-FF-E0-00-00	D-Link Device	IP Surveillance Device
28-10-7B-20-00-00	FF-FF-FF-F0-00-00	D-Link Device	IP Surveillance Device
B0-C5-54-00-00-00	FF-FF-FF-80-00-00	D-Link Device	IP Surveillance Device
F0-7D-68-00-00-00	FF-FF-FF-F0-00-00	D-Link Device	IP Surveillance Device

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду для добавления одного или нескольких OUI Surveillance VLAN. OUI применяется для идентификации трафика видеонаблюдения с помощью функции Surveillance VLAN.

Если MAC-адреса источника полученных пакетов соответствуют любому из шаблонов OUI, полученный пакет распознается как surveillance.

OUI, полученный с устройства видеонаблюдения в Surveillance VLAN, не может совпадать с OUI по умолчанию.

OUI по умолчанию не может быть удален.

Пример

В данном примере показано, как добавить OUI для устройств Surveillance.

```
Switch#configure terminal
Switch(config)#surveillance vlan mac-address 00-01-02-03-00-00 FF-FF-FF-FF-00-00 component-
type vms description user1
Switch(config)#
```

60.5 surveillance vlan onvif-discover-port

Данная команда используется, чтобы настроить номер порта TCP/UDP для отслеживания передачи данных RTSP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

surveillance vlan onvif-discover-port *VALUE*
no surveillance vlan onvif-discover-port

Параметры

VALUE	Укажите номер порта TCP/UDP. Доступные значения: 554; от 1025 до 65535.

По умолчанию

Значение по умолчанию – 554.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда применяется, чтобы настроить номер порта TCP/UDP для отслеживания передачи данных RTSP. IP-камеры и видеорегистраторы с поддержкой протокола ONVIF используют протокол WS-Discovery для поиска других устройств. После обнаружения IP-камер коммутатор может обнаружить видеорегистратор, отслеживая пакеты RTSP, HTTP и HTTPS между видеорегистраторами

и IP-камерами. Данные пакеты нельзя отследить, если порт TCP/UDP не совпадает с номером порта RTSP.

Пример

В данном примере показано, как назначить номер порта TCP/UDP для отслеживания передачи данных RTSP. Указанный номер порта – 2000.

```
Switch# configure terminal
Switch(config)# surveillance vlan onvif-discover-port 2000
Switch(config)#
```

60.6 surveillance vlan onvif-ipc state

Данная команда используется для настройки состояния распознавания IP-камеры при помощи протокола ONVIF. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

surveillance vlan onvif-ipc *IP-ADDRESS* **[mac-address** *MAC-ADDRESS***] state {enable | disable}**

no surveillance vlan onvif-ipc *IP-ADDRESS* **[mac-address** *MAC-ADDRESS***] state**

Параметры

IP-ADDRESS	Укажите IP-адрес IP-камеры.
mac-address *MAC-ADDRESS*	(Опционально.) Укажите MAC-адрес IP-камеры, которая распознается при помощи протокола ONVIF.
enable	Укажите, чтобы включить состояние распознавания IP-камеры при помощи протокола ONVIF.
disable	Укажите, чтобы отключить состояние распознавания IP-камеры при помощи протокола ONVIF.

По умолчанию

По умолчанию функция включена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, для настройки состояния распознавания IP-камеры при помощи протокола ONVIF: может быть использован или только IP-адрес IP-камеры, или одновременно IP-адрес и MAC-адрес IP-камеры. Когда IP-камера ONVIF обнаружена, состояние можно настроить для указанного устройства. Если IP-адреса нескольких IP-камер совпадают, а их MAC-адреса не указаны, это повлияет на состояние распознавания IP-камер.

Данная функция используется для включения/отключения блокировки трафика IP-камеры. Если состояние распознавания IP-камеры на порту отключено, трафик от IP-камеры будет заблокирован.

Пример

В данном примере показано, как включить состояние распознавания IP-камеры с IP-адресом 172.18.60.1.

```
Switch# configure terminal
Switch(config)# surveillance vlan onvif-ipc 172.18.60.1 state enable
Switch(config)#
```

60.7 surveillance vlan onvif-ipc description

Данная команда используется для создания описания IP-камеры, распознанной при помощи протокола ONVIF. Чтобы удалить описание, воспользуйтесь формой **no** этой команды.

surveillance vlan onvif-ipc *IP-ADDRESS* **[mac-address** *MAC-ADDRESS***] description** *TEXT*
no surveillance vlan onvif-ipc *IP-ADDRESS* **[mac-address** *MAC-ADDRESS***] description**

Параметры

IP-ADDRESS	Укажите IP-адрес IP-камеры, распознанной при помощи протокола ONVIF.
mac-address *MAC-ADDRESS*	(Опционально.) Укажите MAC-адрес IP-камеры, которая распознается при помощи протокола ONVIF.
TEXT	Укажите описание IP-камеры, которая распознается при помощи протокола ONVIF. Максимальная длина – 32 символа.

По умолчанию

По умолчанию описание IP-камеры, распознаваемой при помощи протокола ONVIF, отсутствует.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы создать описание IP-камеры, распознанной ONVIF только с помощью IP-адреса IP-камеры или с помощью как IP-адреса, так и MAC-адреса IP-камеры. Если IP-адреса нескольких IP-камер совпадают, а их MAC-адреса не указаны, будет сконфигурировано описание этих IP-камер.

Пример

В данном примере показано, как создать описание IP-камеры с IP-адресом 172.18.60.1. Сконфигурированное описание – «ipc1».

```
Switch# configure terminal
Switch(config)# surveillance vlan onvif-ipc 172.18.60.1 description ipc1
Switch(config)#
```

60.8 surveillance vlan onvif-nvr description

Данная команда используется для создания описания видеорегистратора, распознанного при помощи протокола ONVIF. Чтобы удалить описание, воспользуйтесь формой **no** этой команды.

surveillance vlan onvif-nvr *IP-ADDRESS* **[mac-address** *MAC-ADDRESS***] description** *TEXT*
no surveillance vlan onvif-nvr *IP-ADDRESS* **[mac-address** *MAC-ADDRESS***] description**

Параметры

IP-ADDRESS	Укажите IP-адрес видеорегистратора, распознанного при помощи протокола ONVIF.
mac-address *MAC-ADDRESS*	(Опционально.) Укажите MAC-адрес видеорегистратора, который распознается при помощи протокола ONVIF.
TEXT	Укажите описание видеорегистратора, который распознается при помощи протокола ONVIF. Максимальная длина – 32 символа.

По умолчанию

По умолчанию описание для видеорегистратора, распознанного при помощи протокола ONVIF, отсутствует.

Режим ввода команды

Global Configuration Mode.

Использование команды

Когда видеорегистратор ONVIF распознан, можно настроить описание для указанного устройства.

Используйте данную команду, чтобы создать описание видеорегистратора, распознанного ONVIF только с помощью IP-адреса видеорегистратора или с помощью как IP-адреса, так и MAC-адреса видеорегистратора. Если IP-адреса нескольких видеорегистраторов совпадают, а их MAC-адреса не указаны, будет сконфигурировано описание этих видеорегистраторов.

Пример

В данном примере показано, как создать описание видеорегистратора с IP-адресом 172.18.60.2. Указанное описание – «nvr1».

```
Switch#configure terminal
Switch(config)# surveillance vlan onvif-nvr 172.18.60.2 description nvr1
Switch(config)#
```

60.9 surveillance vlan qos

Данная команда используется, чтобы настроить приоритет CoS для входящего трафика Surveillance VLAN. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

surveillance vlan qos *COS-VALUE*

no surveillance vlan qos

Параметры

COS-VALUE	Укажите приоритет Surveillance VLAN в диапазоне от 0 до 7.

По умолчанию

Значение по умолчанию – 5.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для маркировки CoS пакетов Surveillance, поступающих на порт, на котором включена Surveillance VLAN. Маркировка CoS позволяет отделить трафик Surveillance VLAN от трафика данных по качеству обслуживания.

Пример

В данном примере показано, как указать приоритет 7 для Surveillance VLAN.

```
Switch#configure terminal
Switch(config)# surveillance vlan qos 7
Switch(config)#
```

60.10 show surveillance vlan

Данная команда используется для отображения настроек Surveillance VLAN.

show surveillance vlan [interface [*INTERFACE-ID* **[, | -]]]**
show surveillance vlan device [interface [*INTERFACE-ID* **[, | -]]]**

Параметры

device	Укажите, чтобы отобразить информацию об изученных устройствах Surveillance.
interface *INTERFACE-ID*	(Опционально.) Укажите, чтобы отобразить информацию о Surveillance VLAN на портах.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения настроек Surveillance VLAN.

Для отображения глобальных настроек Surveillance VLAN используйте команду **show surveillance vlan**. Для отображения настроек Surveillance VLAN на интерфейсах используйте команду **show surveillance vlan interface**. Для отображения устройства Surveillance, информация о котором была получена через OUI, введите команду **show surveillance vlan device**.

Пример

В данном примере показано, как отобразить глобальные настройки Surveillance VLAN.

```
Switch#show surveillance vlan

 Surveillance VLAN ID  : 100
 Surveillance VLAN CoS : 5
 Aging Time            : 30 minutes
 ONVIF Discover Port   : 554
 Member Ports          :
 Dynamic Member Ports  :

 Surveillance VLAN OUI :

 OUI Address        Mask               Component Type   Description
 -----------------  -----------------  ---------------  -------------
 28-10-7B-00-00-00  FF-FF-FF-E0-00-00  D-Link Device    IP Surveillance Device
 28-10-7B-20-00-00  FF-FF-FF-F0-00-00  D-Link Device    IP Surveillance Device
 B0-C5-54-00-00-00  FF-FF-FF-80-00-00  D-Link Device    IP Surveillance Device
 F0-7D-68-00-00-00  FF-FF-FF-F0-00-00  D-Link Device    IP Surveillance Device

 Total OUI: 4

Switch#
```

60.11 show surveillance vlan onvif-ipc interface

Данная команда используется для отображения информации об IP-камере на основе протокола ONVIF.

show surveillance vlan onvif-ipc interface [*INTERFACE-ID* **[, | -]] {brief | detail}**

Параметры

INTERFACE-ID	(Опционально.) Укажите порт, информацию о котором необходимо отобразить.

,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
brief	Укажите, чтобы отобразить краткую информацию об IP-камере на основе протокола ONVIF.
detail	Укажите, чтобы отобразить подробную информацию об IP-камере на основе протокола ONVIF.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения краткой или подробной информации об IP-камере на основе протокола ONVIF.

Пример

В данном примере показано, как отобразить краткую информацию об IP-камере на основе протокола ONVIF.

```
Switch#show surveillance vlan onvif-ipc interface eth1/0/1 brief

Interface    : eth1/0/1
IP Address   : 10.90.90.1
MAC Address  : 00-01-02-03-04-05
Model        : P3384-VE
Manufacturer : D-Link
Traffic      : Enabled
Throughput   : 5 Mbps
Description  : P3384-VE

Total Entries: 1

Switch#
```

В данном примере показано, как отобразить подробную информацию об IP-камере на основе протокола ONVIF.

```
Switch#show surveillance vlan onvif-ipc interface eth1/0/1 detail

Interface         : eth1/0/1
IP Address        : 10.90.90.1
MAC Address       : 00-01-02-03-04-05
Model             : P3384-VE
Manufacturer      : D-Link
State             : Enabled
Throughput        : 5 Mbps
Description       : P3384-VE
Protocol          : ONVIF
Power Consumption: 1.9W/15W
PoE               : 802.3af
PoE Status        : Enable

Total Entries: 1

Switch#
```

60.12 show surveillance vlan onvif-nvr interface

Данная команда используется для отображения информации о сетевом видеорегистраторе на основе протокола ONVIF и информации о группе.

show surveillance vlan onvif-nvr interface [*INTERFACE-ID* **[, | -]] [ipc-list]**

Параметры

INTERFACE-ID	(Опционально.) Укажите порт, информацию о котором необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
ipc-list	(Опционально.) Укажите, чтобы отобразить информацию о группе сетевых видеорегистраторов.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения информации о сетевом видеорегистраторе на основе протокола ONVIF и информации о группе. Group ID – это ID группы IP-камер, которые входят в группу сетевых видеорегистраторов. Сетевые видеорегистраторы и IP-камеры, входящие в эту группу, должны иметь один Group ID.

Пример

В данном примере показано, как отобразить информацию о сетевом видеорегистраторе на основе протокола ONVIF.

```
Switch# show surveillance vlan onvif-nvr interface eth1/0/1

Interface    : eth1/0/1
IP Address   : 111.111.111.111
MAC Address  : 00-03-02-03-04-08
IPC Number   : 2
Throughput   : 10 Mbps
Group        : Group 1
Description  : D-Link-NVR

Total Entries: 1

Switch#
```

В данном примере показано, как отобразить информацию о сетевом видеорегистраторе на основе протокола ONVIF, ассоциированным с Group ID «ipc-list».

```
Switch# show surveillance vlan onvif-nvr interface eth1/0/1 ipc-list

Interface IP Address      MAC address       Group    Description
--------- --------------- ----------------- -------- -----------------
1         10.90.90.90.1   00-01-02-03-04-05 1        D-Link-IPC-1
1         10.90.90.90.2   00-01-02-03-04-06 1        D-Link-IPC-2

Total Entries: 2

Switch#
```

61. Команды портов коммутатора

61.1 duplex

Данная команда используется для настройки режима дуплекса на интерфейсе физического порта. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

duplex {full | auto}
no duplex

Параметры

full	Укажите для работы порта в режиме полного дуплекса (Full-Duplex Mode).
auto	Укажите, чтобы режим дуплекса на порту был определен автосогласованием (Auto-Negotiation).

По умолчанию

Для интерфейсов медных портов 10G параметр по умолчанию – **auto**.
Для интерфейсов 10G SFP+ и 25G SFP28 параметр по умолчанию – **full**.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.
Используйте данную команду, чтобы настроить режим дуплекса на физическом порту.

Пример

В данном примере показано, как установить фиксированную скорость 100 Мбит/с и настроить режим дуплекса, определенный автосогласованием, на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#speed 100
Switch(config-if)#duplex auto
Switch(config-if)#
```

61.2 flowcontrol

Данная команда используется для настройки возможности управления потоком (Flow Control) на интерфейсе порта. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

flowcontrol {on | off}
no flowcontrol

Параметры

on	Укажите, чтобы включить на порту отправку или обработку кадров PAUSE, поступающих из удаленных портов.
off	Укажите, чтобы отключить отправку или не получать кадры PAUSE.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

С помощью данной команды можно настроить возможность управления потоком только в программном обеспечении коммутатора. Фактическая операция, выполняемая средствами аппаратного обеспечения, может отличаться от заданной, так как возможность управления потоком настраивается как на текущем, так и на удаленном порту/устройстве.

При установлении фиксированной скорости заданная настройка управления потоком будет окончательной. При установлении скорости, определенной автосогласованием, окончательная примененная настройка управления потоком будет основана на согласовании настроек локального устройства и коммутатора. В данном случае настройка управления потоком осуществляется с помощью локального устройства.

Пример

В данном примере показано, как включить управление потоком на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#flowcontrol on
Switch(config-if)#
```

61.3 mdix

Данная команда используется для настройки состояния MDIX порта. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

mdix {auto | normal | cross}

no mdix

Параметры

auto	Укажите, чтобы включить режим Auto-MDIX Mode.
normal	Укажите, чтобы включить режим Normal Mode.
cross	Укажите, чтобы включить режим Cross Mode.

По умолчанию

Параметр по умолчанию – **auto**.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда неприменима на порту, к которому подключен оптоволоконный кабель.

Пример

В данном примере показано, как настроить режим Auto-MDIX Mode на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mdix auto
Switch(config-if)#
```

61.4 speed

Данная команда используется для настройки скорости интерфейса физического порта. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

speed {100 | 1000 | 10giga | 25giga | auto [*SPEED-LIST***]}**
no speed

Параметры

100	Укажите, чтобы установить скорость 100 Мбит/с.
1000	Укажите, чтобы установить скорость 1000 Мбит/с.
10giga	Укажите, чтобы установить скорость 10 Гбит/с.
25giga	Укажите, чтобы установить скорость 25 Гбит/с.
auto	Укажите, чтобы скорость и управление потоком с оборудованием на противоположной стороне были заданы при помощи автосогласования.
SPEED-LIST	(Опционально.) Укажите список скоростей, применяемых для автосогласования. Возможны следующие скорости: **100**, **1000,** и/или **10giga**. Если используются несколько скоростей, необходимо отделить их запятой (,). Если список скоростей не указан, будут анонсированы все варианты скорости.

По умолчанию

Для интерфейсов медных портов 10G и портов 10G SFP+ по умолчанию скорость определяется автоматически.
Для интерфейсов 25G SFP28 по умолчанию устанавливается фиксированная скорость 25 Гбит/с.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.

Автосогласование должно быть включено на медных портах 10G. Эта функция не поддерживается на оптоволоконных портах 25G. На коммутаторах модели DXS-1210-28T порты 25-28 должны работать с одной скоростью.

Примечание: функция FEC не поддерживается на портах SFP28 25 Гбит/с. Если подключение между одним коммутатором и другим – не принадлежащим к серии DXS-1210 – устройством прервано, необходимо отключить функцию FEC на удаленном коммутаторе.

Пример

В данном примере показано, как на интерфейсе Ethernet 1/0/1 включить автосогласование, при котором будут использоваться только скорости 100 Мбит/с или 1000 Мбит/с.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# speed auto 100,1000
Switch(config-if)#
```

62. Команды управления системными файлами

62.1 boot config

Данная команда используется для указания конфигурационного файла, который будет использован при следующем запуске устройства.

boot config {Config1 | Config2}

Параметры

Config1	Укажите, чтобы использовать Config1 в качестве конфигурационного файла при следующем запуске устройства.
Config2	Укажите, чтобы использовать Config2 в качестве конфигурационного файла при следующем запуске устройства.

По умолчанию

По умолчанию используется файл Config1.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы указать конфигурационный файл, который будет использован при следующем запуске устройства. При отсутствии конфигурационного файла устройство вернется к настройкам по умолчанию.

Пример

В данном примере показано, как указать конфигурационный файл «Config2», который будет использован при следующем запуске устройства.

```
Switch#configure terminal
Switch(config)#boot config Config2
Switch(config)#
```

62.2 boot image

Данная команда используется для указания файла образа, который будет использован при следующем запуске устройства.

boot image [check] {Image1 | Image2}

Параметры

check	(Опционально.) Укажите данный параметр для отображения информации о программном обеспечении для указанного файла (номер версии и описание модели).

Image1	Укажите, чтобы использовать Image1 в качестве файла образа для загрузки.
Image2	Укажите, чтобы использовать Image2 в качестве файла образа для загрузки.

По умолчанию

По умолчанию в качестве файла образа для загрузки используется Image1.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы указать файл образа, который будет использован при следующем запуске устройства. После проверки и утверждения системой модели и контрольной суммы файл образа будет допущен.

Используйте параметр **check**, чтобы проверить, может ли быть допущен указанный файл образа для загрузки. Настройка команды **boot image** будет сохранена в энергонезависимой памяти NVRAM, благодаря которой сохраненный файл будет использован при следующем запуске устройства.

Пример

В данном примере показано, как указать файл под именем «Image1» в качестве файла образа для загрузки.

```
Switch#configure terminal
Switch(config)#boot image Image1
Switch(config)#
```

62.3 clear running-config

Данная команда используется для удаления текущей конфигурации системы (running configuration).

clear running-config

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы удалить конфигурацию системы, сохраненную в DRAM-память. Данные конфигурации вернутся к настройкам по умолчанию. Перед использованием данной команды сохраните резервную копию конфигурации с помощью команды **copy** или выгрузите профиль конфигурации на TFTP-сервер.

При удалении настроек конфигурации системы стираются параметры IP. Таким образом, все существующие удаленные подключения будут прерваны. После применения данной команды необходимо настроить IP-адрес через локальную консоль.

Пример

В данном примере показано, как удалить текущую конфигурацию системы.

```
Switch#clear running-config

This command will clear the system's configuration to the factory
default settings, including the IP address.
Clear running configuration? (y/n) [n] y

Switch#
```

62.4 reset system

Данная команда используется для сброса системы и удаления ранее сохраненной конфигурации с дальнейшей перезагрузкой коммутатора.

reset system

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду для удаления конфигурации системы. Данные конфигурации вернутся к настройкам по умолчанию, будет создан соответствующий конфигурационный файл загрузки, затем будет выполнен перезапуск коммутатора. Перед использованием данной команды сохраните резервную копию конфигурации с помощью команды **copy** или выгрузите профиль конфигурации на TFTP-сервер.

Пример

В данном примере показано, как сбросить систему и вернуться к настройкам по умолчанию.

```
Switch# reset system

This command will clear the system's configuration to the factory
default settings, including the IP address.
Clear system configuration, save, reboot? (y/n) [n]  y

Saving configurations and logs to NV-RAM..... Done.
Please wait, the switch is rebooting...
```

62.5 configure replace

Данная команда используется для замены текущей конфигурации указанным конфигурационным файлом.

configure replace {{tftp: //*LOCATION/FILENAME* | flash: {Config1 | Config2}} [force]

Параметры

tftp:	Укажите конфигурационный файл с TFTP-сервера.
//LOCATION/FILENAME	Укажите URL конфигурационного файла на TFTP-сервере.
flash:	Укажите конфигурационный файл из NVRAM устройства.
Config1	Укажите Config1 в качестве файла конфигурации загрузки.
Config2	Укажите Config2 в качестве файла конфигурации загрузки.
force	(Опционально.) Укажите, чтобы принудительно применить команду без дополнительного подтверждения.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду, чтобы заменить текущую конфигурацию указанным конфигурационным файлом. Текущая конфигурация будет удалена перед применением указанной конфигурации.

Примечание: при выполнении данной команды текущая конфигурация полностью меняется на конфигурацию указанного файла. В указанном конфигурационном файле должна быть представлена полная конфигурация, а не частичная.

Перед использованием данной команды сохраните резервную копию конфигурации с помощью команды **copy** или выгрузите профиль конфигурации на TFTP-сервер.

Пример

В данном примере показано, как заменить текущую конфигурацию файлом «config.cfg», загруженным с TFTP-сервера.

```
Switch#configure replace tftp: //10.0.0.66/config.cfg

This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. [y/n]:  y

 Accessing tftp://10.0.0.66/config.cfg...
 Transmission start...
 Transmission finished, file length 45422 bytes.
 Executing script file config.cfg ......
 Executing done

Switch#
```

В примере ниже показано, как заменить текущую конфигурацию файлом «Config1», хранящимся в NVRAM. Команда выполняется принудительно без дополнительного подтверждения.

```
Switch#configure replace flash: Config1 force

 Executing script file Config1 ......
 Executing done

Switch#
```

62.6 copy

Данная команда используется для копирования файлов.

copy *SOURCE-URL DESTINATION-URL*
copy *SOURCE-URL* **tftp: [//***LOCATION/DESTINATION-URL***]**
copy {tftp: [//*LOCATION/SOURCE-URL***]** *DESTINATION-URL*

Параметры

SOURCE-URL	Укажите URL источника исходного файла, который необходимо скопировать. Особые формы URL представлены следующими ключевыми словами: Укажите **startup-config** в качестве URL источника, чтобы выгрузить конфигурацию, которая будет применена после запуска коммутатора, сохранить ее как файл в файловой системе или использовать в качестве текущей конфигурации. Укажите **running-config** в качестве URL источника, чтобы выгрузить текущую конфигурацию, сохранить ее в качестве загрузочной конфигурации или как файл в файловой системе.

	Укажите **flash**: **[***PATH-FILE-NAME***]** в качестве URL источника, чтобы скопировать исходный файл в файловую систему. Укажите **log** в качестве URL, чтобы выгрузить системный журнал на TFTP-сервер. Укажите **attack-log** в качестве URL источника, чтобы выгрузить журнал атак.
DESTINATION-URL	Укажите URL назначения скопированного файла. Особые формы URL представлены следующими ключевыми словами: Укажите **running-config** в качестве URL назначения, чтобы применить конфигурацию к текущей конфигурации. Укажите **startup-config** в качестве URL назначения, чтобы сохранить конфигурацию, которую необходимо применить при следующем запуске. Текущая конфигурация будет сохранена в NVRAM, а имя файла будет совпадать с именем файла, указанным при использовании команды **boot config**. Укажите **flash: {Image1 | Image2 | Config1 | Config2}** в качестве URL назначения, чтобы указать имя копируемого файла в файловой системе. Укажите **flash: certificate-key** *STRING* в качестве URL назначения, чтобы указать имя сертификата назначения или файл ключа, который необходимо скопировать в файловую систему. Укажите **flash: private-key** *STRING* в качестве URL назначения, чтобы указать имя закрытого ключа, который необходимо скопировать в файловую систему. Укажите **flash: public-key** *STRING* в качестве URL назначения, чтобы указать имя ключа общего пользования, который необходимо скопировать в файловую систему.
LOCATION	(Опционально.) Укажите IPv4-адрес или IPv6-адрес TFTP-сервера.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Используйте данную команду для копирования файлов в файловую систему, загрузки/выгрузки конфигурационного файла или файла образа. Чтобы выгрузить текущую конфигурацию или сохранить ее в качестве загрузочной конфигурации, укажите **running-config** в качестве URL источника. Чтобы сохранить текущую конфигурацию в качестве загрузочной конфигурации, укажите **startup-config** в качестве URL назначения.

Если в качестве назначения указана загрузочная конфигурация, файл исходника будет скопирован в файл, указанный в команде **boot config**. Исходный файл загрузочной конфигурации будет перезаписан.

Чтобы применить необходимый конфигурационный файл к текущей конфигурации, при использовании команды **copy** укажите **running-config** в качестве URL назначения. Данный конфигурационный файл будет сразу же применен при помощи метода increment. Указанная конфигурация будет объединена с текущей конфигурацией. Текущая конфигурация будет удалена только после применения указанной конфигурации.

Если в качестве источника указан системный журнал, а в качестве назначения указан URL, текущий системный журнал будет скопирован на указанный URL.

Чтобы отобразить файл на удаленном TFTP-сервере, необходимо использовать URL с префиксом «tftp: //» .

Чтобы загрузить образ программного обеспечения, используйте команду **copy tftp:** // для загрузки файла с TFTP-сервера в файловую систему. Чтобы указать данный файл в качестве файла образа для загрузки, используйте команду **boot image**.

Пример

В данном примере показано, как настроить на коммутаторе текущую конфигурацию, загруженную с TFTP-сервера 10.1.1.254, используя метод increment. Имя конфигурационного файла: switch-config.cfg.

```
Switch#copy tftp: //10.1.1.254/switch-config.cfg running-config

Address of remote host [10.1.1.254]?
Source filename [switch-config.cfg]?
Destination filename running-config? [y/n]:  y

 Accessing tftp://10.1.1.254/switch-config.cfg...
 Transmission start...
 Transmission finished, file length 29974 bytes.
 Executing script file switch-config.cfg ......
 Executing done

Switch#
```

В примере ниже показано, как выгрузить текущую конфигурацию на TFTP-сервер для хранения.

```
Switch#copy running-config tftp: //10.1.1.254/switch-config.cfg

Address of remote host [10.1.1.254]?
Destination filename [switch-config.cfg]?
 Accessing tftp://10.5.2.101/switch-config.cfg...
 Transmission start...
 Transmission finished, file length 28999 bytes.

Switch#
```

В следующем примере показано, как сохранить текущую конфигурацию во flash-память и использовать ее при следующем запуске устройства.

```
Switch#copy running-config startup-config

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM..... Done.

Switch#
```

Ниже показан пример немедленного сохранения файла «Config2» в NVRAM с использованием метода increment.

```
Switch#copy flash: Config2 running-config

Source filename [Config2]?
Destination filename running-config? [y/n]:  y

 Executing script file Config2 ......
 Executing done

Switch#
```

В нижеприведенном примере показано, как загрузить файл образа с TFTP-сервера.

```
Switch#copy tftp: //10.1.1.254/runtime.had flash: Image1

Address of remote host [10.1.1.254]?
Source filename [dxs-1210.had]?
Destination filename [Image1]?
 Accessing tftp://10.1.1.254/runtime.had...
 Transmission start...
 Transmission finished, file length 8315060 bytes.
 Please wait, programming flash.............. Done.

Switch#
```

62.7 reboot

Данная команда используется для перезагрузки коммутатора.

reboot [force_agree]

Параметры

force_agree	(Опционально.) Укажите, чтобы перезагрузить коммутатор без дополнительного подтверждения.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для перезагрузки коммутатора.

Пример

В данном примере показано, как перезагрузить коммутатор.

```
Switch# reboot force_agree

Please wait, the switch is rebooting...
```

62.8 show boot

Данная команда используется для отображения настроек конфигурационного файла и загрузочного образа.

show boot

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения настроек конфигурационного файла и загрузочного образа.

Пример

В данном примере показано, как отобразить информацию о загрузке системы.

```
Switch#show boot

 Boot image: /c:/Image1
 Boot config: /c:/Config1


Switch#
```

62.9 show running-config

Данная команда используется для отображения команд текущего конфигурационного файла.

show running-config [effective | all] [interface *INTERFACE-ID* **| vlan** *VLAN-ID***]**

Параметры

effective	(Опционально.) Укажите, чтобы отобразить настройки команды, которые влияют на работу устройства. Например, если STP отключен, будет отображена команда **disable stp**. Все другие настройки STP (настройки более низкого уровня) не отображаются. Настройки нижнего уровня будут отображаться только в том случае, если включена настройка верхнего уровня. Если этот параметр не выбран, будут отображены только измененные настройки, отличные от настроек по умолчанию.
all	(Опционально.) Укажите, чтобы отобразить все команды конфигурации, включая команды, которые соответствуют параметрам по умолчанию. Если этот параметр не выбран, будут отображены только измененные настройки, отличные от настроек по умолчанию.
interface *INTERFACE-ID*	(Опционально.) Укажите интерфейс, который необходимо отобразить.
vlan *VLAN-ID*	(Опционально.) Укажите VLAN, которую необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения текущей конфигурации.

Пример

В данном примере показано, как отобразить содержимое текущего конфигурационного файла.

```
Switch#show running-config
Building configuration...

Current configuration : 1291 bytes

!----------------------------------------------------------------------------
!             DXS-1210-28T 10 Gigabit Ethernet Smart Managed Switch
!                                Configuration
!
!                            Firmware: Build 1.00.021
!           Copyright(C) 2020 D-Link Corporation. All rights reserved.
!----------------------------------------------------------------------------

line console
!
line telnet
!
line ssh
!
interface Ethernet1/0/1
!
interface Ethernet1/0/2
!
interface Ethernet1/0/3
!
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a Alll
```

62.10 show startup-config

Данная команда используется для отображения содержимого конфигурационного загрузочного файла.

show startup-config

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения настроек конфигурации, с помощью которых система будет инициализирована.

Пример

В данном примере показано, как отобразить содержимое конфигурационного загрузочного файла.

```
Switch#show startup-config

!----------------------------------------------------------------------------
!             DXS-1210-28T 10 Gigabit Ethernet Smart Managed Switch
!                                Configuration
!
!                             Firmware: Build 1.00.021
!           Copyright(C) 2020 D-Link Corporation. All rights reserved.
!----------------------------------------------------------------------------

ip http timeout-policy idle 36000
!
line console
 session-timeout 0
!
line telnet
!
line ssh
!
interface Ethernet1/0/1
!
interface Ethernet1/0/2
!
interface Ethernet1/0/3
!
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

63. Команды System Log

63.1 clear logging

Данная команда используется для удаления сообщений из внутреннего буфера.

clear logging

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Команда позволяет удалить все сообщения из внутреннего буфера.

Пример

В данном примере показано, как удалить все сообщения из внутреннего буфера.

```
Switch#clear logging
Clear logging? (y/n) [n]  y
Switch#
```

63.2 logging on

Данная команда используется для включения логирования системных сообщений. Используйте форму **no**, чтобы отключить логирование системных сообщений.

logging on
no logging on

Параметры

Нет.

По умолчанию

По умолчанию опция включена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы включить / отключить логирование системных сообщений.

Данная команда регистрирует отладочные сообщения (debug) и сообщения об ошибках (error) в системном журнале (логе). Процесс сохранения сообщений идет асинхронно процессам, генерирующим данные сообщения. Используйте форму **no** этой команды для отключения данной функции.

Процесс логирования контролирует распределение сообщений по нескольким направлениям, таким как буфер логирования, консоль или syslog-сервер. Для включения или отключения функции логирования для каждого направления индивидуально можно использовать команды **logging buffered**, **logging server** и **logging console**. Однако если команда **logging on** отключена, сообщения по данным направлениям отправляться не будут. Если команда **logging on** включена, одновременно с ней будет активирована команда **logging buffered**.

Пример

В данном примере показано, как включить логирование системных сообщений.

```
Switch#configure terminal
Switch(config)#logging on
WARNING: The command takes effect and the logging buffered is enabled at the same time.
Switch(config)#
```

63.3 logging buffered

Данная команда используется для включения логирования системных сообщений во внутренний буфер. При использовании формы **no** команда отключит логирование системных сообщений во внутренний буфер. Используйте команду **default logging buffered**, чтобы вернуться к настройкам по умолчанию.

logging buffered [severity {*SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [discriminator** *NAME***] [write-delay {***SECONDS* **| infinite}]**

no logging buffered

default logging buffered

Параметры

SEVERITY-LEVEL	(Опционально.) Укажите уровень важности системных сообщений. Сообщения с заданным уровнем важности или выше передаются во внутренний буфер. Доступны значения от 0 до 7, где 0 – наиболее высокий уровень важности. Если значение не указано, по умолчанию используется уровень важности warnings (**4**).
SEVERITY-NAME	(Опционально.) Укажите название уровня важности системных сообщений: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational**, **debugging**.
discriminator	(Опционально.) Укажите discriminator для фильтрации сообщений, отправляемых во внутренний буфер.
write-delay *SECONDS*	(Опционально.) Укажите, чтобы отключить периодическое сохранение содержимого буфера журнала во FLASH-память.

По умолчанию

По умолчанию используется уровень важности warning (4).

Режим ввода команды

Global Configuration Mode.

Использование команды

Системные сообщения можно передать в локальный буфер и другие точки назначения. Перед отправкой в другие точки назначения сообщения должны поступить в локальный буфер.

Команда не применяется, если указанный discriminator не существует. В этом случае применяются настройки по умолчанию.

Укажите уровень важности сообщений для ограничения системных сообщений, логируемых в буфер (это позволит уменьшить количество зарегистрированных сообщений). Сообщения указанного уровня или выше логируются в буфер. При заполнении буфера старые записи удаляются, чтобы освободить место для новых сообщений.

Содержимое буфера периодически сохраняется во flash-память, чтобы при перезагрузке сообщения можно было восстановить. При необходимости можно задать интервал для сохранения записей из буфера во flash-память. При перезагрузке содержимое сообщений, сохраняемых во flash-память, будет перезагружено в буфер логирования.

Пример

В данном примере показано, как включить логирование сообщений в буфер и ограничить логирование сообщений с уровнем важности errors или выше.

```
Switch#configure terminal
Switch(config)#logging buffered severity errors
Switch(config)#
```

63.4 logging console

Данная команда используется для включения логирования системных сообщений в локальной консоли. При использовании формы **no** команда отключит логирование сообщений в локальной консоли и вернет настройки по умолчанию.

logging console [severity {*SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [discriminator** *NAME***]**
no logging console

Параметры

SEVERITY-LEVEL	(Опционально.) Укажите уровень важности системных сообщений. Сообщения с заданным уровнем важности или выше передаются во внутренний буфер. Доступны значения от 0 до 7, где 0 – наиболее высокий уровень важности. Уровни важности сообщений: **0** – emergencies – чрезвычайная ситуация, система не работоспособна,

	1 – alerts – тревога, система требует немедленного вмешательства, **2** – critical – состояние системы критическое, **3** – errors – сообщения об ошибках, **4** – warnings – предупреждения о возможных проблемах, **5** – notifications – уведомления о нормальных, но важных событиях, **6** – informational – информационные сообщения, **7** – debugging – отладочные сообщения. Если значение не указано, по умолчанию используется уровень важности warnings (**4**).
SEVERITY-NAME	(Опционально.) Укажите название уровня важности системных сообщений: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).
discriminator	(Опционально.) Укажите discriminator для фильтрации сообщений, отправляемых в локальный буфер.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Системные сообщения можно логировать в локальный буфер сообщений, локальную консоль или другие точки назначения. Перед отправкой на консоль сообщения должны предварительно поступить в локальный буфер.

Команда не применяется, если указанный discriminator не существует. В этом случае будут применяться настройки по умолчанию.

Укажите уровень важности сообщений для ограничения системных сообщений, логируемых в консоли. Сообщения указанного уровня или выше будут логироваться в локальную консоль.

Пример

В данном примере показано, как включить логирование сообщений в локальную консоль и ограничить логирование сообщений с уровнем важности errors или выше.

```
Switch#configure terminal
Switch(config)#logging console severity errors
Switch(config)#
```

63.5 logging discriminator

Данная команда используется при создании discriminator для дальнейшей фильтрации сообщений syslog, отправляемых в различные точки назначения. При использовании формы **no** команда удалит discriminator.

logging discriminator *NAME* **[facility {drops** *STRING* **| includes** *STRING***}] [severity {drops** *SEVERITY-LIST* **| includes** *SEVERITY-LIST***}]**

no logging discriminator *NAME*

Параметры

NAME	Укажите имя discriminator.
facility	(Опционально.) Укажите, чтобы использовать под-фильтр на основе категории facility.
STRING	Укажите одно или более имен facility. Если используется несколько имен, они должны быть разделены запятой без пробелов.
includes	Укажите для включения совпадающих сообщений. Несовпадающие сообщения будут фильтроваться.
drops	Укажите для фильтрации совпадающих сообщений.
severity	(Опционально.) Укажите под-фильтр на основе совпадений с уровнем важности.
SEVERITY- LIST	Укажите список уровней важности для фильтрации или включения.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Настраивается существующий параметр discriminator. При вводе команды предыдущие настройки будут заменены новыми. Ассоциируйте discriminator с командами **logging buffered** и **logging server**.

Пример

В данном примере показано, как создать discriminator с именем «buffer-filter», указывающим два подфильтра: один на основе уровня важности, а другой на основе facility.

```
Switch#configure terminal
Switch(config)#logging discriminator buffer-filter facility includes STP severity includes 1-
4,6
Switch(config)#
```

63.6 logging server

Данная команда используется для включения логирования системных сообщений на указанный syslog-сервер. При использовании формы **no** команда удалит syslog-сервер с указанным адресом из списка syslog-серверов.

logging server {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [severity {***SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [facility {***FACILITY-NUM* **|** *FACILITY-NAME***}] [discriminator** *NAME***] [port** *UDP-PORT***]**

no logging server {*IP-ADDRESS* **|** *IPV6-ADDRESS***}**

Параметры

IP-ADDRESS	Укажите IP-адрес syslog-сервера.
IPV6-ADDRESS	Укажите IPv6-адрес серверного узла логирования.
SEVERITY-LEVEL	(Опционально.) Укажите уровень важности системных сообщений. Сообщения с заданным уровнем важности или выше передаются в буфер сообщений. Доступны значения от 0 до 7, где 0 – наиболее высокий уровень важности. Если значение не указано, по умолчанию используется уровень важности warnings (**4**).
SEVERITY-NAME	(Опционально.) Укажите название уровня важности системных сообщений. Имена уровней важности: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational**, **debugging**.
FACILITY-NUM	(Опционально.) Укажите десятичное значение от 0 до 23 для facility. Если значение не указано, по умолчанию будет использоваться local7 (**23**). Для более подробной информации обратитесь к параграфу Использование команды.
FACILITY-NAME	(Опционально.) Укажите имя facility. Если значение не указано, по умолчанию будет использоваться **local7** (23). Для более подробной информации обратитесь к параграфу Использование команды.
discriminator *NAME*	(Опционально.) Укажите для фильтрации сообщений на сервер логирования согласно настройке discriminator.
port *UDP-PORT*	(Опционально.) Укажите номер порта UDP, который будет использоваться сервером syslog. Доступен диапазон значений от 1024 до 65535, а также 514 (распространенный порт IANA). Если значение не указано, номер UDP-порта по умолчанию – 514.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Системные сообщения можно логировать в локальный буфер сообщений, на локальную консоль или удаленные узлы. Перед отправкой на сервер логирования сообщения должны поступить в локальный буфер сообщений.

Ниже представлена таблица значений Facility.

Числовой код	Facility
0	Сообщения ядра
1	Сообщения уровня пользователя
2	Система почты
3	Системные daemon
4	Сообщения системы безопасности/авторизации
5	Сообщения, генерируемые SYSLOG
6	Подсистема Line Printer
7	Подсистема сетевых новостей
8	Подсистема UUCP
9	Clock daemon
10	Сообщения системы безопасности/авторизации
11	FTP daemon
12	Подсистема NTP
13	Аудит логирования
14	Предупреждение логирования
15	Clock daemon (note 2)
16	Локальное использование 0 (local0)
17	Локальное использование 1 (local1)
18	Локальное использование 2 (local2)
19	Локальное использование 3 (local3)
20	Локальное использование 4 (local4)
21	Локальное использование 5 (local5)
22	Локальное использование 6 (local6)
23	Локальное использование 7 (local7)

Пример

В данном примере показано, как включить логирование системных сообщений с уровнем важности выше warnings на удаленном узле 20.3.3.3.

```
Switch#configure terminal
Switch(config)#logging server  20.3.3.3 severity warnings
Switch(config)#
```

63.7 show logging

Данная команда используется для просмотра системных сообщений, хранящихся во внутреннем буфере.

show logging [all | [*REF-SEQ***] [+** *NN* **| -** *NN***]]**

Параметры

all	Укажите для вывода всех записей журнала, начиная с последних.
REF-SEQ	Укажите порядковый номер, с которого начнется вывод записей.
+ *NN*	Укажите количество сообщений, которое необходимо отобразить после указанного порядкового номера. Если номер не указан, отображение начинается с самого раннего сообщения в буфере.
- *NN*	Укажите количество сообщений, которое необходимо отобразить до указанного номера. Если номер не указан, отображение начинается с последнего сообщения в буфере.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Команда используется для просмотра сообщений, хранящихся во внутреннем буфере.

Каждое сохраненное в буфер сообщение соотносится с определенным порядковым номером. При регистрации сообщению назначается порядковый номер, начиная с 1. При достижении значения 100000 нумерация вновь начнется с 1.

Если задается количество сообщений, которые необходимо отобразить после указанного порядкового номера, то вывод сообщений начнется с более ранних записей. Если задается количество сообщений, которые предшествуют указанному порядковому номеру, то вывод сообщений начнется с более поздних записей.

Если команда введена без опций, система выводит 200 записей, начиная с последнего сообщения.

Пример

В данном примере показано, как отобразить сообщения в локальном буфере сообщений.

```
Switch# show logging

Total number of buffered messages: 2

#2 2013-08-02 16:37:36 INFO(6) Logout through Console (Username: Anonymous)
#1 2013-08-02 16:35:54 INFO(6) Port eth1/0/1 link up, 1000Mbps FULL duplex

switch#
```

63.8 show attack-logging

Данная команда используется для просмотра зарегистрированных сообщений об атаках.

show attack-logging [index *INDEX***]**

Параметры

index *INDEX*	(Опционально.) Укажите список порядковых номеров записей, которые необходимо отобразить. Если значение не указано, отображаться будут все записи из журнала атак.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для просмотра сообщений об атаках в журнале. К таким сообщениям относятся записи, связанные с функционалом DOS и port-security. В этом случае может генерироваться большое количество подобных сообщений, из-за чего в системе быстро заканчивается память для хранения записей журнала. Чтобы этого избежать, в системный журнал сохраняется только первое сообщение данного типа, генерируемое каждую минуту, а остальные хранятся в отдельной таблице с именем attack log (журнал атак).

Пример

В данном примере показано, как отобразить первое зарегистрированное сообщение об атаке.

```
Switch#show attack-logging

Attack log messages (total number:0)


Switch#
```

63.9 clear attack-logging

Данная команда используется для удаления сообщений об атаках.

clear attack-logging {all}

Параметры

all	Укажите для удаления всех записей.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для удаления сообщений об атаках.

Пример

В данном примере показано, как удалить все логированные сообщения об атаках.

```
Switch#clear attack-logging all
Switch#
```

64. Команды времени и SNTP

64.1 clock set

Данная команда используется для установки системного времени вручную.

clock set *HH:MM:SS DAY MONTH YEAR*

Параметры

HH:MM:SS	Укажите текущее время: часы (24-часовой формат), минуты и секунды.
DAY	Укажите текущий день месяца.
MONTH	Укажите текущий месяц (jan, feb, mar, apr и т. д.).
YEAR	Укажите текущий год без сокращений.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если система синхронизируется с помощью любого действующего внешнего механизма синхронизации, такого как SNTP, необходимо установить системное время. Используйте данную команду, если другие источники времени недоступны. Время, указанное в данной команде, принадлежит к часовому поясу, заданному конфигурацией команды **clock timezone**. Если устройство поддерживает функцию RTC (часы реального времени), время синхронизируется с RTC. Настроенные часы не будут сохранены в файле конфигурации.

Сервер SNTP является основным источником времени: даже если системное время было настроено вручную, при подключении к серверу SNTP время будет синхронизировано с его показателями.

Пример

В данном примере показано, как вручную установить системное время на 6:00, 4 июля 2020 г.

```
Switch# clock set 18:00:00 4 jul 2020
Switch#
```

64.2 clock summer-time

Данная команда используется для настройки автоматического перехода на летнее время. Чтобы отключить автоматический переход на летнее время, воспользуйтесь формой **no** этой команды.

clock summer-time recurring *WEEK DAY MONTH HH:MM WEEK DAY MONTH HH:MM* **[***OFFSET***]**

clock summer-time date *DATE MONTH YEAR HH:MM DATE MONTH YEAR HH:MM* **[***OFFSET***]**

no clock summer-time

Параметры

recurring	Укажите дату начала и окончания летнего времени (день недели и месяц).
date	Укажите точную дату начала и окончания летнего времени.
WEEK	Укажите номер недели месяца (от 1 до 4) или слово «last», с помощью которого будет указана последняя неделя месяца.
DAY	Укажите день недели (sun, mon и т. д.).
DATE	Укажите день месяца (от 1 до 31).
MONTH	Укажите текущий месяц (jan, feb, mar, apr и т. д.).
YEAR	Укажите года, чтобы задать необходимый интервал для применения перехода на летнее время.
HH:MM	Укажите время (24-часовой формат) в часах и минутах.
OFFSET	(Опционально.) Укажите количество минут, которое нужно добавить при переходе на летнее время. Значение по умолчанию – 60. Диапазон смещения – 30, 60, 90 и 120 минут.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы перейти на летнее время автоматически. У команды две формы: первая – повторяющаяся (**recurring**), которая используется для указания даты начала и окончания летнего времени (день недели и месяц); вторая – форма даты (**date**), которая используется для указания определенного числа месяца.

Первая часть данных команд указывает на начало летнего времени, а вторая – на конец.

Пример

В данном примере показано, как назначить начало летнего времени на 2 часа ночи первого воскресенья июня и конец на 2 часа ночи последнего воскресенья октября.

```
Switch# configure terminal
Switch(config)# clock summer-time recurring 1 sun jun 2:00 last sun oct 2:00
Switch(config)#
```

64.3 clock timezone

Данная команда используется для настройки и отображения часового пояса. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

clock timezone {+ | -} *HOURS-OFFSET* **[***MINUTES-OFFSET***]**
no clock timezone

Параметры

+ | -	Укажите количество часов, которое необходимо прибавить к UTC.
-	Укажите количество часов, которое необходимо вычесть из UTC.
HOURS-OFFSET	Укажите разницу во времени с UTC в часах.
MINUTES-OFFSET	(Опционально.) Укажите разницу во времени с UTC в минутах.

По умолчанию

Часовой пояс по умолчанию – UTC.

Режим ввода команды

Global Configuration Mode.

Использование команды

Время, полученное с сервера SNTP, синхронизируется с форматом UTC. При настройке местного времени учитывается формат UTC, часовой пояс и настройки перехода на летнее время.

Пример

В данном примере показано, как настроить часовой пояс PST (Северноамериканское Тихоокеанское Стандартное Время), который на 8 часов опережает время UTC.

```
Switch#configure terminal
Switch(config)#clock timezone - 8
Switch(config)#
```

64.4 show clock

Данная команда используется для отображения информации о времени и дате.

show clock

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Также данная команда применяется для отображения источника времени. Возможные источники: «No Time Source» (источник времени отсутствует) или «SNTP».

Пример

В данном примере показано, как отобразить текущее время.

```
Switch# show clock

     Current Time Source   : System Clock
     Current Time          : 05:56:45, 2000-01-01
     Time Zone             : UTC +00:00
     Daylight Saving Time  : Disabled

Switch#
```

64.5 show sntp

Данная команда используется для отображения информации о сервере SNTP.

show sntp

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применяется для отображения информации о сервере SNTP.

Пример

В данном примере показано, как отобразить информацию об SNTP.

```
Switch#show sntp

SNTP Status               : Enabled
SNTP Poll Interval        : 720 sec

SNTP Server Status:

SNTP Server                                    Version Last Receive
---------------------------------------------- ------- ---------------
172.31.151.44                                  3       00:00:29 Synced
172:31:151:24::44                              ------- ---------------
FE80::41A2:ACB6:9B9E:C5D4%vlan40               ------- ---------------
---------------------------------------------- ------- ---------------
Total Entries:3


Switch#
```

64.6 sntp server

Данная команда используется для синхронизации системного времени с сервером SNTP. Чтобы удалить сервер из списка серверов SNTP, воспользуйтесь формой **no** этой команды.

sntp server {*IP-ADDRESS* **|** *IPV6-ADDRESS***}**
no sntp server {*IP-ADDRESS* **|** *IPV6-ADDRESS***}**

Параметры

IP-ADDRESS	Укажите IP-адрес сервера, который обеспечивает синхронизацию времени.
IPV6-ADDRESS	Укажите IPv6-адрес сервера времени.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

SNTP – это упрощенная клиентская версия NTP. В отличие от NTP, SNTP может получать время только от серверов NTP; его нельзя использовать для предоставления времени другим системам. SNTP обеспечивает время с погрешностью 100 миллисекунд от точного времени, но, в отличии от NTP, не обеспечивает сложных механизмов фильтрации и статистической обработки. Кроме того, SNTP не проверяет подлинность трафика, хотя с помощью настройки расширенного списка доступа можно обеспечить определённую степень защиты.

Чтобы создать несколько серверов SNTP, введите данную команду несколько раз, используя разные IP-адреса серверов SNTP.

Используйте форму **no**, чтобы удалить запись сервера SNTP. При удалении записи укажите точную

информацию, введенную при первом подключении. Время, полученное с сервера SNTP, синхронизируется с форматом UTC.

Пример

В данном примере показано, как синхронизировать системное время с сервером SNTP с IP-адресом 192.168.22.44.

```
Switch#configure terminal
Switch(config)#sntp server 192.168.22.44
Switch(config)#
```

64.7 sntp enable

Данная команда используется для включения функции SNTP. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

sntp enable
no sntp enable

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда применяется для включения/отключения функции SNTP.

Пример

В данном примере показано, как включить функцию SNTP.

```
Switch#configure terminal
Switch(config)#sntp enable
Switch(config)#
```

64.8 sntp interval

Данная команда используется для настройки интервала синхронизации часов SNTP-клиента с сервером. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

sntp interval *SECONDS*
no sntp interval

Параметры

SECONDS	Укажите интервал синхронизации в диапазоне от 30 до 99999 секунд.

По умолчанию

Значение по умолчанию – 720 секунд.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для настройки интервала опроса (Polling Interval).

Пример

В данном примере показано, как настроить интервал опроса. Указанное значение – 100 секунд.

```
Switch#configure terminal
Switch(config)#sntp interval 100
Switch(config)#
```

65. Команды временного диапазона

65.1 periodic

Данная команда используется для указания профиля диапазона времени. Чтобы удалить указанный временной диапазон, воспользуйтесь формой **no** этой команды.

periodic {daily *HH:MM* **to** *HH:MM* **| weekly** *WEEKLY-DAY HH:MM* **to [***WEEKLY-DAY***]** *HH:MM***}**
no periodic {daily *HH:MM* **to** *HH:MM* **| weekly** *WEEKLY-DAY HH:MM* **to [***WEEKLY-DAY***]** *HH:MM***}**

Параметры

daily *HH:MM* **to** *HH:MM*	Укажите время в формате ЧЧ:ММ (например, 18:30).
weekly *WEEKLY-DAY HH***:***MM* **to [***WEEKLY-DAY***]** *HH***:***MM*	Укажите день недели (monday, tuesday, wednesday, thursday, friday, saturday, sunday) и время в формате ЧЧ:ММ. Конечный день недели, совпадающий с начальным, можно не указывать.

По умолчанию

Нет.

Режим ввода команды

Time-range Configuration Mode.

Использование команды

Новый период может частично совпадать с предыдущим. Если начало и завершение нового периода соответствуют началу и завершению предыдущего периода, будет отображено сообщение об ошибке и новый период не будет задан. При удалении необходимо полностью указать заданный ранее период. Если период указан не полностью или указано сразу несколько периодов, будет отображено сообщение об ошибке.

Пример

В данном примере показано, как создать временной интервал, включающий промежутки с 09:00 до 12:00 ежедневно и с 00:00 субботы до 00:00 понедельника, а также как удалить период с 09:00 до 12:00 ежедневно.

```
Switch#configure terminal
Switch(config)#time-range rdtime
Switch(config-time-range)#periodic daily 9:00 to 12:00
Switch(config-time-range)#periodic weekly saturday 00:00 to monday 00:00
Switch(config-time-range)#no periodic daily 9:00 to 12:00
Switch(config-time-range)#
```

65.2 show time-range

Данная команда используется для отображения конфигурации профиля диапазона времени.

show time-range [*NAME***]**

Параметры

NAME	(Опционально.) Укажите имя профиля диапазона времени для отображения.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если параметр не указан, будут отображены все настроенные профили диапазона времени.

Пример

В данном примере показано, как отобразить все настроенные профили.

```
Switch# show time-range

Time Range Profile: rdtime
Daily 09:00 to 12:00
Weekly Saturday 00:00 to Monday 00:00

Time Range Profile: lunchtime
Daily 12:00 to 13:00

Total Entries: 2

Switch#
```

65.3 time-range

Данная команда используется для указания профиля диапазона времени и входа в режим Time-Range Configuration Mode. Чтобы удалить временной диапазон, воспользуйтесь формой **no** этой команды.

time-range *NAME*
no time-range *NAME*

Параметры

NAME	Укажите имя профиля диапазона времени, который необходимо настроить. Максимальное количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы войти в режим Time-Range Configuration Mode. Команду следует применять перед командой **periodic**, используемой для указания временного диапазона. Если временной диапазон создается без какой-либо настройки, это означает, что для данного временного диапазона нет активного периода.

Пример

В данном примере показано, как войти в режим Time-Range Configuration Mode для профиля диапазона времени с именем «rdtime».

```
Switch#configure terminal
Switch(config)#time-range rdtime
Switch(config-time-range)#
```

66. Команды Traffic Segmentation

66.1 show traffic-segmentation forward

Данная команда используется для отображения конфигурации Traffic Segmentation.

show traffic-segmentation forward [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейсы для отображения.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и port-channel.

Если параметр не указан, будет отображена конфигурация Traffic Segmentation для всех портов.

Пример

В данном примере показано, как отобразить конфигурацию Traffic Segmentation для интерфейса Ethernet 1/0/1.

```
Switch# show traffic-segmentation forward interface eth1/0/1

Interface        Forwarding Domain
-------------    ------------------------------------------------------------
eth1/0/1         eth1/0/2,1/0/4-1/0/6

Total Entries: 1

Switch#
```

66.2 traffic-segmentation forward

Данная команда используется для ограничения продвижения пакетов в L2 домене, приходящих на настроенный порт. Чтобы удалить ограничение продвижения пакетов в L2 домене, воспользуйтесь формой **no** этой команды.

traffic-segmentation forward interface *INTERFACE-ID* **[, | -]**
no traffic-segmentation forward interface *INTERFACE-ID* **[, | -]**

Параметры

INTERFACE-ID	Укажите разрешенные интерфейсы необходимых физических портов.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.

Если домен продвижения пакетов задан Traffic Segmentation, то пакеты, получаемые портом, будут ограничены пакетами, отправленными интерфейсами внутри заданного L2 домена. Если ограничение продвижения пакетов в домене L2 не указано, то получение портом пакетов не ограничено.

Команду **traffic-segmentation forward** можно применять несколько раз. Все последующие интерфейсы будут добавлены в список участников домена. Используйте форму **no**, чтобы удалить указанный интерфейс из данного списка.

В список участников Traffic Segmentation могут входить различные типы интерфейсов, например, порт и port-channel в одном домене. Если интерфейсы, указанные командой, включают port-channel, все порты-участники данного port-channel будут добавлены в список участников домена.

Если домен продвижения пакетов для интерфейса не указан, то ограничений на продвижение пакетов на указанном порту нет.

Пример

В данном примере показано, как настроить Traffic Segmentation и ограничить домен лавинной рассылки для интерфейса Ethernet 1/0/1. Установленное ограничение: от интерфейса Ethernet 1/0/3 до Ethernet 1/0/6.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#traffic-segmentation forward interface eth1/0/3-6
Switch(config-if)#
```

67. Команды Transport Layer Security (TLS)

67.1 no certificate

Данная команда используется для удаления импортированного сертификата.

no certificate *NAME*

Параметры

NAME	Укажите имя сертификата, который необходимо удалить.

По умолчанию

Нет.

Режим ввода команды

Certificate Chain Configuration Mode.

Использование команды

Используйте команду **show crypto pki trustpoints**, чтобы отобразить список имен импортированных сертификатов. Затем в команде no certificate укажите импортированные сертификаты доверенной точки (trust point), которые необходимо удалить. Если указанный сертификат является локальным, соответствующий закрытый ключ также будет удален. При удалении закрытого ключа будет отображено предупреждающее сообщение.

Пример

В данном примере показано, как удалить импортированный сертификат. Имя сертификата – tongken.ca. Доверенная точка (trust point) – gaa.

```
Switch#show crypto pki trustpoints

Trustpoint Name        : gaa (primary)
  Imported certificates:
    CA                 : tongken.ca
    local certificate  : webserver.crt
    local private key  : webserver.prv

Switch#configure terminal
Switch(config)#crypto pki certificate chain gaa
Switch(config-cert-chain)#no certificate tongken.ca
Switch(config-cert-chain)#
```

67.2 crypto pki import pem

Данная команда используется для импорта сертификата ЦС (Центра Сертификации/Certificate Authority) или сертификата коммутатора и ключей в доверенной точке (trust point) из файлов в формате PEM (Privacy-Enhanced Mail).

crypto pki import *TRUSTPOINT* **pem** *FILE-SYSTEM***:/[***DIRECTORY***/]***FILE-NAME* **[password** *PASSWORD-PHRASE***] {ca | local | both}**

crypto pki import *TRUSTPOINT* **pem tftp: //***IP-ADDRESS***/[***DIRECTORY***/]** *FILE-NAME* **[password** *PASSWORD-PHRASE***] {ca | local | both}**

Параметры

TRUSTPOINT	Укажите имя trust point, которое ассоциировано с импортированными сертификатами и парами ключей.
FILE-SYSTEM	Укажите файловую систему для сертификатов и пар ключей. После указанной файловой системы необходимо использовать двоеточие «:». Например, «flash:» указывает, что файловая система является локальной.
DIRECTORY	(Опционально.) Укажите имя каталога для импорта сертификатов и пар ключей. Возможен импорт в коммутатор или на TFTP-сервер.
FILE-NAME	Укажите имя сертификатов и пар ключей, которые необходимо импортировать. По умолчанию к имени сертификата ЦС добавляется .ca, к закрытому ключу – .prv, к сертификату – .crt.
password *PASSWORD-PHRASE*	(Опционально.) Укажите зашифрованную фразу пароля для отмены шифрования при импорте закрытых ключей. Максимальное количество символов в строке – 64. Если фраза пароля не указана, используется пустая строка.
tftp	Укажите URL источника для сетевого TFTP-сервера.
IP-ADDRESS	Укажите IP-адрес TFTP-сервера.
ca	Укажите, чтобы импортировать только сертификат ЦС.
local	Укажите, чтобы импортировать локальный сертификат и пары ключей.
both	Укажите, чтобы импортировать сертификат ЦС, локальный сертификат и пары ключей.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда позволяет администраторам импортировать сертификаты и пары ключей в файлы в формате PEM.

Соответствующие сертификаты и пары ключей необходимо импортировать в коммутатор в соответствии с желаемым алгоритмом обмена ключами. Сертификаты/пары ключей RSA и DSA

должны быть импортированы для RSA и DHS-DSS соответственно. Сертификаты и ключи RSA и DSA несовместимы. SSL-клиент, имеющий только сертификат и ключ RSA, не может установить соединение с SSL-сервером, у которого есть только сертификат и ключ DSA.

Импортированные сертификат (-ы) могут образовывать цепочку, которая устанавливает последовательность доверенных сертификатов: от сертификата узла до корневого сертификата ЦС. Доверенная точка ЦС (trust point CA) – это центр сертификации (Certificate Authority, CA), настроенный на коммутаторе в качестве доверенного ЦС. Любой полученный сертификат узла будет принят, если он подтвержден локальным доверенным ЦС или его подчиненными.

Если указанной доверенной точки не существует, появится сообщение об ошибке.

Пример

В данном примере показано, как импортировать файлы сертификатов (ЦС и локальных) и пары ключей в доверенную точку (trust point) «TP1» через TFTP.

```
Switch#configure terminal
Switch(config)#crypto pki import TP1 pem tftp: //10.1.1.2/name/msca password abcd1234 both

% Importing CA certificate...
Destination filename [name/msca.ca]?
Reading file from tftp://10.1.1.2/name/msca.ca
Loading name/msca.ca from 10.1.1.2 (via eth1/0/5):!
[OK - 1082 bytes]

% Importing private key PEM file...
Reading file from tftp://10.1.1.2/name/msca.prv
Loading name/msca.prv from 10.1.1.2 (via eth1/0/5):!
[OK - 573 bytes]

% Importing certificate PEM file...
Reading file from tftp://10.1.1.2/name/msca.crt
Loading name/msca.crt from 10.1.1.2 (via eth1/0/5):!
[OK - 1289 bytes]
% PEM files import succeeded.

Switch(config)#
```

67.3 crypto pki trustpoint

Данная команда используется для настройки доверенной точки trust point на коммутаторе. Чтобы удалить все сертификаты и пары ключей, ассоциированные с определенной trust point, воспользуйтесь формой **no** этой команды.

crypto pki trustpoint *NAME*
no crypto pki trustpoint *NAME*

Параметры

NAME	Укажите имя доверенной точки (trust point).

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить доверенную точку (trust point), которая может выступать в качестве самоподтвержденного корневого центра сертификации или подчиненного ЦС. При использовании данной команды будет выполнен вход в режим CA-Trust-Point Configuration Mode.

Пример

В данном примере показано, как настроить trust point «TP1» и указать ее в качестве основной.

```
Switch#configure terminal
Switch(config)#crypto pki trustpoint TP1
Switch(ca-trustpoint)#primary
Switch(ca-trustpoint)#
```

67.4 crypto pki certificate chain

Данная команда используется для входа в режим Certificate Chain Configuration Mode.

crypto pki certificate chain *NAME*

Параметры

NAME	Укажите имя доверенной точки (trust point).

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы войти в режим Certificate Chain Configuration Mode. Если указанного имени доверенной точки (trust point) не существует, будет отображено сообщение об ошибке.

Пример

В данном примере показано, как войти в режим Certificate Chain Configuration Mode.

```
Switch#configure terminal
Switch(config)#crypto pki certificate chain TP1
Switch(trustpoint)#
```

67.5 primary

Данная команда используется для назначения указанной доверенной точки (trust point) в качестве основной trust point коммутатора. Для отмены назначения воспользуйтесь формой **no** этой команды.

primary
no primary

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

CA-Trust-Point Configuration Mode.

Использование команды

Используйте данную команду, чтобы указать доверенную точку (trust point) в качестве основной. Указанная trust point будет использоваться по умолчанию, если система не может определить, какую trust point центра сертификации необходимо использовать. В качестве основной может быть указана только одна trust point. После указания trust point в качестве основной, предыдущая trust point будет перезаписана.

Пример

В данном примере показано, как настроить trust point «TP1» в качестве основной.

```
Switch#configure terminal
Switch(config)#crypto pki trustpoint TP1
Switch(ca-trustpoint)#primary
Switch(ca-trustpoint)#
```

67.6 show crypto pki trustpoints

Данная команда используется для отображения trust point, настроенных на коммутаторе.

show crypto pki trustpoints [*TRUSTPOINT***]**

Параметры

TRUSTPOINT	(Опционально.) Укажите имя trust point для отображения.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если параметры не указаны, будут отображены все trust point.

Пример

В данном примере показано, как отобразить все trust point.

```
Switch#show crypto pki trustpoints

Trustpoint Name        : TP1 (primary)
  Imported certificates:
    CA                 : tongken.ca
    local certificate  : webserver.crt
    local private key  : webserver.prv

Trustpoint Name        : TP2
  Imported certificates:
    CA                 : chunagtel.ca
    local certificate  : openflow.crt
    local private key  : openflow.prv

Switch#
```

67.7 show ssl-service-policy

Данная команда используется для отображения политики SSL service policy.

show ssl-service-policy [*POLICY-NAME***]**

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики SSL service policy.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Если параметры не указаны, будут отображены все SSL service policy.

Пример

В данном примере показано, как отобразить все SSL service policy.

```
Switch# show ssl-service-policy

SSL Policy Name        : policyForHttp
  Enabled Versions :
        TLS 1.0
        TLS 1.1
        TLS 1.2
  Enabled CipherSuites :
        DHE_DSS_WITH_3DES_EDE_CBC_SHA,
        RSA_WITH_3DES_EDE_CBC_SHA,
        RSA_WITH_RC4_128_SHA,
        RSA_WITH_RC4_128_MD5,
        RSA_EXPORT_WITH_RC4_40_MD5
        RSA_WITH_AES_128_CBC_SHA
        RSA_WITH_AES_256_CBC_SHA
        RSA_WITH_AES_128_CBC_SHA256
        RSA_WITH_AES_256_CBC_SHA256
        DHE_DSS_WITH_AES_256_CBC_SHA
        DHE_RSA_WITH_AES_256_CBC_SHA
  Session Cache Timeout: 600
  Secure Trustpoint    : ggg

SSL Policy Name        : policyForFTP
  Enabled Versions :
        TLS 1.0
        TLS 1.1
        TLS 1.2
  Enabled CipherSuites :
        RSA_WITH_RC4_128_MD5,
        RSA_EXPORT_WITH_RC4_40_MD5
  Session Cache Timeout: 1200
  Secure Trustpoint    : domain2

Switch#
```

67.8 ssl-service-policy

Данная команда используется для настройки политики SSL service policy. Для удаления политики SSL service policy воспользуйтесь формой **no** этой команды.

ssl-service-policy *POLICY-NAME* **[version [***VERSION***] | ciphersuite [***CIPHERSUITE***] | secure-trustpoint** *TRUSTPOINT* **| session-cache-timeout** *TIME-OUT***]**

no ssl-service-policy *POLICY-NAME* **[version [***VERSION***] | ciphersuite [***CIPHERSUITE***] | secure-trustpoint** *TRUSTPOINT* **| session-cache-timeout** *TIME-OUT***]**

Параметры

POLICY-NAME	Укажите имя политики SSL service policy.
version *VERSION*	(Опционально.) Укажите версию TLS. • **tls1.0** – укажите, чтобы использовать TLS версии 1.0 в

	качестве политики SSL service policy. • **tls1.1** – укажите, чтобы использовать TLS версии 1.1 в качестве политики SSL service policy. • **tls1.2** – укажите, чтобы использовать TLS версии 1.2 в качестве политики SSL service policy.
ciphersuite *CIPHERSUITE*	(Опционально.) Укажите шифрование cipher suite, которое будет использовать служба безопасности при установлении соединения с удаленным узлом. Если шифрование Cipher Suite не настроено, клиент и сервер SSL согласовывают наиболее подходящее шифрование из списка доступных Cipher Suite. Будет выбрано шифрование, которое поддерживается и SSL-клиентом, и SSL-сервером. Возможно использование нескольких Cipher Suite. Для отключения выбранных Cipher Suite воспользуйтесь формой **no**. • Чтобы использовать обмен ключами DH с шифрованием 3DES-EDE-CBC и SHA для дайджеста сообщений, укажите **dhe-dss-3des-ede-cbc-sha**. • Чтобы использовать обмен ключами RSA с шифрованием 3DES и DES-EDE3-CBC и Secure Hash Algorithm (SHA) для дайджеста сообщений, укажите **rsa-3des-ede-cbc-sha**. • Чтобы использовать обмен ключами RSA с 128-битным шифрованием RC4 и SHA для дайджеста сообщений, укажите **rsa-rc4-128-sha**. • Чтобы использовать обмен ключами RSA с 128-битным шифрованием RC4 и Message Digest 5 (MD5) для дайджеста сообщений, укажите **rsa-rc4-128-md5**. • Чтобы использовать обмен ключами RSA EXPORT с 40-битным шифрованием RC4 и MD5 для дайджеста сообщений, укажите **rsa-export-rc4-40-md5**. • Чтобы использовать обмен ключами RSA с 128-битным шифрованием AES и SHA для дайджеста сообщений, укажите **rsa-aes-128-cbc-sha**. • Чтобы использовать обмен ключами RSA с 256-битным шифрованием AES и SHA для дайджеста сообщений, укажите **rsa-aes-256-cbc-sha**. • Чтобы использовать обмен ключами RSA с 128-битным шифрованием AES и 256-битным SHA для дайджеста сообщений, укажите **rsa-aes-128-cbc-sha256**. • Чтобы использовать обмен ключами RSA с 256-битным шифрованием AES и 256-битным SHA для дайджеста сообщений, укажите **rsa-aes-256-cbc-sha256**. • Чтобы использовать обмен ключами DH с 256-битным шифрованием AES и SHA для дайджеста сообщений по методу DSS, укажите **dhe-dss-aes-256-cbc-sha**.

	• Чтобы использовать обмен ключами DH с 256-битным шифрованием AES и SHA для дайджеста сообщений по методу RSA, укажите **dhe-rsa-aes-256-cbc-sha**.
secure-trustpoint *TRUSTPOINT*	(Опционально.) Укажите имя доверенной точки (trust point), которую необходимо использовать при установке SSL. Если данный параметр не указан, будет использоваться trust point, выступающая в роли основной. Если основная trust point не указана, будет использоваться встроенный сертификат/пары ключей. Используйте форму **no** этой команды, чтобы отменить указанные trust point и использовать встроенный сертификат/пары ключей.
session-cache-timeout *TIME-OUT*	(Опционально.) Укажите значение тайм-аута в секундах для информации, хранящейся в кэше SSL-сессий. Диапазон значений: от 60 до 86400 секунд. Если данный параметр не указан, тайм-аут кэша сессий по умолчанию составляет 600 секунд. Используйте форму **no** этой команды, чтобы вернуть настройки по умолчанию для тайм-аута кэша SSL-сессий.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить политику SSL service policy.

Пример

В данном примере показано, как настроить политику SSL service policy, которая ассоциирована с trust point «TP1». Настроенная политика SSL service policy – «ssl-server».

```
Switch#configure terminal
Switch(config)#ssl-service-policy ssl-server secure-trustpoint TP1
Switch(config)#
```

67.9 crypto pki certificate generate

Данная команда используется для генерирования нового самоподписанного сертификата.

crypto pki certificate generate

Параметры

Нет.

По умолчанию

По умолчанию коммутатор автоматически генерирует случайный встроенный сертификат.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду, чтобы сгенерировать новый самоподписанный сертификат. Данная команда применяется независимо от того, сгенерирован ли встроенный самоподписанный сертификат или нет. Коммутатор сгенерирует новый самоподписанный сертификат автоматически, если после загрузки коммутатора сертификат не был обнаружен.

Сертификат, который был сгенерирован с помощью данной команды, не влияет на сертификаты, загруженные пользователем.

Примечание: в данной команде поддерживается только самоподписанный сертификат RSA с длиной ключа 2048.

Пример

В данном примере показано, как сгенерировать новый самоподписанный сертификат.

```
Switch#configure terminal
Switch(config)#crypto pki certificate generate

Start generating key ...
Start generating self-signed certificate ...
Done.
Switch(config)#
```

68. Команды Virtual LAN (VLAN)

68.1 acceptable-frame

Данная команда используется для настройки допустимых типов кадров на порту. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

acceptable-frame {tagged-only | untagged-only | admit-all}
no acceptable-frame

Параметры

tagged-only	Допускаются только тегированные кадры.
untagged-only	Допускаются только нетегированные кадры.
admit-all	Допускаются все кадры.

По умолчанию

Для режима access VLAN mode опцией по умолчанию является **untagged-only**.
Для режима other VLAN mode опцией по умолчанию является **admit-all**.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда используется для настройки допустимых типов кадров на порту**.**

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 на прием только тегированных кадров **tagged-only**.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#acceptable-frame tagged-only
Switch(config-if)#
```

68.2 ingress-checking

Данная команда используется для включения проверки входящих кадров, получаемых портом. Используйте форму **no** для отключения проверки.

ingress-checking
no ingress-checking

Параметры

Нет.

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Используйте данную команду для включения проверки входящих кадров, получаемых интерфейсом. При включенной проверке пакет будет отброшен, если принимающий порт не является участником VLAN, классифицированной для получаемого пакета.

Пример

В данном примере показано, как настроить проверку входящего трафика для включенного интерфейса Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ingress-checking
Switch(config-if)#
```

68.3 show vlan

Данная команда используется для отображения параметров для всех настроенных VLAN или одной VLAN на коммутаторе.

show vlan [*VLAN-ID* **[, | -] | interface [***INTERFACE-ID* **[, | -]]]**

Параметры

VLAN-ID	(Опционально.) Укажите список VLAN для отображения информации о портах-участниках. Если VLAN не указана, то отображаются все VLAN. Допустимый диапазон: от 1 до 4094.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
interface *INTERFACE-ID*	(Опционально.) Укажите порт для отображения настроек VLAN.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для отображения параметров одной или всех настроенных на коммутаторе VLAN.

Пример

В данном примере показано, как отобразить все текущие записи VLAN.

```
Switch#show vlan

 VLAN 1
   Name : default
   Description :
   Tagged Member Ports   :
   Untagged Member Ports : eth1/0/1-1/0/28

 Total Entries : 1

Switch#
```

В данном примере показано, как отобразить информацию о PVID, проверке входящих пакетов и допустимых типах кадров для интерфейсов Ethernet 1/0/1-1/0/2.

```
Switch#show vlan interface eth1/0/1-2

 eth1/0/1
   VLAN Mode             : Hybrid
   Native VLAN           : 1
   Hybrid Untagged VLAN  : 1
   Hybrid Tagged VLAN    :
   Ingress Checking      : Enabled
   Acceptable Frame Type : Admit-All

 eth1/0/2
   VLAN Mode             : Hybrid
   Native VLAN           : 1
   Hybrid Untagged VLAN  : 1
   Hybrid Tagged VLAN    :
   Ingress Checking      : Enabled
   Acceptable Frame Type : Admit-All


Switch#
```

68.4 switchport access vlan

Данная команда используется, чтобы указать access VLAN для интерфейса. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

switchport access vlan *VLAN-ID*
no switchport access vlan

Параметры

VLAN-ID	Укажите access VLAN интерфейса.

По умолчанию

По умолчанию access VLAN является VLAN 1.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда вступает в силу, когда интерфейс настроен в режиме доступа (access mode). VLAN, указанная в качестве access VLAN, не должна обязательно существовать для настройки команды.

Можно указать только одну access VLAN. Следующая команда перезаписывает предыдущую.

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 в режиме доступа (access mode) с access VLAN 1000.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 1000
Switch(config-if)#
```

68.5 switchport hybrid allowed vlan

Данная команда используется для указания тегированных или нетегированных VLAN для гибридного порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

switchport hybrid allowed vlan {[add] {tagged | untagged} | remove} *VLAN-ID* **[, | -]**
no switchport hybrid allowed vlan

Параметры

add	(Опционально.) Укажите порт, который будет добавлен в указанную(-ые) VLAN.
remove	Укажите порт, который будет удален из указанной(-ых) VLAN.
tagged	Укажите порт в качестве тегированного для указанной(-ых) VLAN.
untagged	Укажите порт в качестве нетегированного для указанной(-ых) VLAN.

VLAN-ID	Укажите список разрешенных VLAN или список VLAN, который будет добавлен или удален из списка разрешенных VLAN. Если опция не задана, указанный список VLAN перезапишет список разрешенных VLAN.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию гибридный порт является нетегированным членом VLAN 1.

Режим ввода команды

Interface Configuration Mode.

Использование команды

При многократном использовании команды hybrid VLAN с разными VLAN ID порт может стать тегированным или нетегированным участником нескольких VLAN.

Когда разрешенная VLAN указана только как VLAN ID, следующая команда перезапишет предыдущую команду. Если новый нетегированный разрешенный список VLAN частично совпадает с текущим списком тегированных разрешенных VLAN, то совпадающая часть будет изменена на нетегированную разрешенную VLAN. С другой стороны, если новый список тегированных разрешенных VLAN частично совпадает с текущим списком нетегированных разрешенных VLAN, то совпадающая часть будет изменена на тегированную разрешенную VLAN. В силу вступает последняя заданная команда. Необязательно создавать VLAN, чтобы настроить данную команду.

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 в качестве тегированного порта VLAN 1000 и нетегированного порта VLAN 2000 и 3000.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode hybrid
Switch(config-if)#switchport hybrid allowed vlan add tagged 1000
Switch(config-if)#switchport hybrid allowed vlan add untagged 2000,3000
Switch(config-if)#
```

68.6 switchport hybrid native vlan

Данная команда используется для указания native VLAN ID гибридного порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

switchport hybrid native vlan *VLAN-ID*

no switchport hybrid native vlan

Параметры

VLAN-ID	Native VLAN гибридного порта.

По умолчанию

По умолчанию native VLAN гибридного порта является VLAN 1.

Режим ввода команды

Interface Configuration Mode.

Использование команды

При настройке привязки гибридного порта к его native VLAN используйте команду **switchport hybrid allowed vlan**, чтобы добавить native VLAN в список разрешенных VLAN. Указанная VLAN не должна обязательно существовать для применения этой команды. Команда вступает в силу, если интерфейс настроен в гибридном режиме.

Пример

В данном примере показано, как настроить Ethernet 1/0/1 в качестве гибридного интерфейса и задать PVID со значением 20.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode hybrid
Switch(config-if)#switchport hybrid allowed vlan add untagged 1000,20
Switch(config-if)#switchport hybrid native vlan 20
Switch(config-if)#
```

68.7 switchport mode

Данная команда используется для настройки режима работы порта в VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

switchport mode {access | hybrid | trunk}
no switchport mode

Параметры

access	Укажите порт в качестве порта доступа.
hybrid	Укажите порт в качестве гибридного порта.
trunk	Укажите порт в качестве trunk-порта.

По умолчанию

По умолчанию установлена опция **hybrid**.

Режим ввода команды

Interface Configuration Mode.

Использование команды

В режиме **access** порт выступает в качестве нетегированного участника access VLAN, заданной для данного порта. В режиме **hybrid** порт может быть нетегированным или тегированным участником всех настроенных VLAN.

В режиме **trunk** этот порт является либо тегированным, либо нетегированным участником его native VLAN и может быть тегированным участником других настроенных VLAN. Цель trunk-порта – поддержка соединения switch-to-switch.

При изменении режима работы порта настройки, связанные с VLAN и ассоциированные с предыдущим режимом, будут утеряны.

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 в качестве trunk-порта.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
```

68.8 switchport trunk allowed vlan

Данная команда используется для настройки VLAN, которым разрешено получать и отправлять трафик на указанный интерфейс в тегированном формате. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

switchport trunk allowed vlan {all | [add | remove | except] *VLAN-ID* **[, | -]}**
no switchport trunk allowed vlan

Параметры

all	Указывает, что на интерфейсе разрешены все VLAN.
add	(Опционально.) Укажите, чтобы добавить указанный список VLAN в список разрешенных VLAN.
remove	(Опционально.) Укажите, чтобы удалить указанный список VLAN из списка разрешенных VLAN.
except	(Опционально.) Указывает, что разрешены все VLAN, за исключением VLAN, находящихся в списке исключений.
VLAN-ID	Укажите список разрешенных VLAN или список VLAN, которые должны быть добавлены в список разрешенных VLAN или удалены из него.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.

-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию все VLAN разрешены.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Данная команда вступает в силу, только когда интерфейс настроен в режиме trunk. Если VLAN разрешена на trunk-порту, то порт станет тегированным участником VLAN. Когда для разрешенной VLAN установлена опция **all**, то порт будет автоматически добавлен во все VLAN, созданные системой.

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 в качестве тегированного участника VLAN 1000.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 1000
Switch(config-if)#
```

68.9 switchport trunk native vlan

Данная команда используется для указания native VLAN ID интерфейса в режиме trunk. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

switchport trunk native vlan {*VLAN-ID* **| tag}**
no switchport trunk native vlan [tag]

Параметры

VLAN-ID	Native VLAN для trunk-порта.
tag	Включение режима тегирования (tagging mode) native VLAN.

По умолчанию

По умолчанию задана native VLAN 1, режим – нетегированный.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Команда вступает в силу, только когда интерфейс настроен в режиме trunk. Если native VLAN trunk-порта настроен в тегированном режиме (tagged mode), обычно допустимый тип кадров порта должен быть настроен как «tagged-only», чтобы принимать только тегированные кадры. Если trunk-порт работает в нетегированном режиме (untagged mode) для native VLAN, передавая нетегированный пакет для native VLAN и тегированные пакеты для всех остальных VLAN, допустимые типы кадров порта должны быть настроены как «admit-all» для корректной работы.

Указанная VLAN не должна обязательно существовать для настройки команды.

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 в качестве интерфейса trunk и native VLAN 20.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 20
Switch(config-if)#
```

68.10 vlan

Данная команда используется для добавления VLAN и входа в режим VLAN configuration mode. Используйте форму **no** для удаления VLAN.

vlan *VLAN-ID* **[, | -]**
no vlan *VLAN-ID* **[, | -]**

Параметры

VLAN-ID	Идентификатор VLAN, которая должны быть добавлена, удалена или настроена. Корректный диапазон VLAN ID: от 1 до 4094. VLAN ID 1 не может быть удален.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

VLAN ID 1 существует в системе в качестве VLAN по умолчанию.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте команду глобальной настройки **vlan** для создания VLAN. Ввод команды **vlan** с VLAN ID обеспечивает вход в режим настройки VLAN (VLAN configuration mode). Ввод VLAN ID существующей

VLAN не создает новую VLAN, но разрешает пользователю изменить параметры VLAN для указанной VLAN. Когда пользователь вводит VLAN ID новой VLAN, VLAN будет создана автоматически.

Используйте команду **no vlan** для удаления VLAN. VLAN по умолчанию не может быть удалена. Если удаленная VLAN является access VLAN порта, то access VLAN порта будет сброшена в VLAN 1.

Пример

В данном примере показано, как добавить новые VLAN, назначив новые VLAN с VLAN ID от 1000 до 1005.

```
Switch#configure terminal
Switch(config)#vlan 1000-1005
Switch(config-vlan)#
```

68.11 name

Данная команда используется для указания имени VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

name *VLAN-NAME*
no name

Параметры

VLAN-NAME	Имя VLAN (макс. 32 символа). Имя VLAN должно быть уникальным в административном домене.

По умолчанию

По умолчанию именем VLAN является VLANx, где x – четыре цифры номера VLAN, включая начальные нули.

Режим ввода команды

VLAN Configuration Mode.

Использование команды

Используйте данную команду, чтобы задать имя VLAN. Имя VLAN должно быть уникальным в административном домене.

Пример

В данном примере показано, как задать имя «admin-vlan» для VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#name admin-vlan
Switch(config-vlan)#
```

69. Команды Voice VLAN

69.1 voice vlan

Данная команда используется для глобального включения функции Voice VLAN и её настройки. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

voice vlan *VLAN-ID*
no voice vlan

Параметры

VLAN-ID	Укажите ID Voice VLAN в диапазоне от 2 до 4094.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду для глобального включения функции Voice VLAN и ее настройки. На коммутаторе может быть настроена только одна Voice VLAN.

Для включения функции Voice VLAN необходимо применить команду **voice vlan** в режиме Global Configuration Mode и команду **voice vlan enable** в режиме Interface Configuration Mode.

При включении на порту функции Voice VLAN полученные VoIP-пакеты будут перенаправлены в данную Voice VLAN. При соответствии MAC-адресов источника пакетов адресам уникального идентификатора организации (OUI), настроенным при помощи команды **voice vlan mac-address**, полученные пакеты распознаются как VoIP-пакеты.

Настройки Voice VLAN можно применить только к уже существующей VLAN. Настроенную Voice VLAN нельзя удалить с помощью команды **no vlan**.

Пример

В данном примере показано, как включить функцию Voice VLAN и настроить VLAN 1000 в качестве Voice VLAN.

```
Switch#configure terminal
Switch(config)#voice vlan 1000
Switch(config)#
```

69.2 voice vlan aging

Данная команда используется для настройки времени устаревания (Aging Time) для устаревших динамических member-портов Voice VLAN. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

voice vlan aging *MINUTES*
no voice vlan aging

Параметры

MINUTES	Укажите время устаревания Voice VLAN в диапазоне от 1 до 65535 минут.

По умолчанию

Значение по умолчанию – 720 минут.

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду для настройки времени устаревания для VoIP-устройства и автоматически изученных member-портов Voice VLAN. Когда последнее VoIP-устройство, подключенное к порту, перестает отправлять трафик и MAC-адрес данного устройства устаревает в FDB, запускается таймер времени устаревания Voice VLAN. По истечении данного времени порт будет удален из Voice VLAN. Если VoIP-трафик возобновляется в течение времени устаревания, таймер будет отменен.

Пример

В данном примере показано, как настроить время устаревания Voice VLAN. Указанное значение – 30 минут.

```
Switch#configure terminal
Switch(config)#voice vlan aging 30
Switch(config)#
```

69.3 voice vlan enable

Данная команда используется для включения функции Voice VLAN на портах. Чтобы отключить данную функцию на портах, воспользуйтесь формой **no** этой команды.

voice vlan enable
no voice vlan enable

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Используйте команду **voice vlan** в режиме Global Configuration Mode и **voice vlan enable** в режиме Interface Configuration Mode, чтобы включить функцию Voice VLAN на портах доступа или гибридных портах.

Пример

В данном примере показано, как включить функцию Voice VLAN на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#voice vlan enable
Switch(config-if)#
```

69.4 voice vlan mac-address

Данная команда используется для добавления определенного пользователем OUI (уникального идентификатора организации) VoIP-устройства. Чтобы удалить определенный пользователем OUI VoIP-устройства, воспользуйтесь формой **no** этой команды.

voice vlan mac-address *MAC-ADDRESS MASK* **[description** *TEXT***]**

no voice vlan mac-address *MAC-ADDRESS MASK*

Параметры

MAC-ADDRESS	Укажите MAC-адрес OUI.
MASK	Укажите соответствующую битовую маску MAC-адреса OUI.
description *TEXT*	(Опционально.) Укажите описание определенного пользователем OUI. Максимальное количество символов – 32.

По умолчанию

OUI по умолчанию указаны в следующей таблице:

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

Режим ввода команды

Global Configuration Mode.

Использование команды

Используйте данную команду для добавления определенного пользователем OUI VoIP-устройства. OUI используется для идентификации VoIP-трафика с помощью функции Voice VLAN. Если MAC-адреса источника полученных пакетов соответствуют любому из шаблонов OUI, полученные пакеты распознаются как VoIP-пакеты.

Определенный пользователем OUI не может совпадать с OUI по умолчанию. OUI по умолчанию не может быть удален.

Пример

В данном примере показано, как добавить определенный пользователем OUI для VoIP-устройства.

```
Switch#configure terminal
Switch(config)#voice vlan mac-address 00-02-03-00-00-00 FF-FF-FF-00-00-00 description User1
Switch(config)#
```

69.5 voice vlan mode

Данная команда используется для включения автоматического изучения порта в качестве member-порта Voice VLAN. Чтобы отключить автоматическое изучение, воспользуйтесь формой **no** этой команды.

voice vlan mode {manual | auto {tag | untag}}
no voice vlan mode

Параметры

manual	Укажите, чтобы настроить членство Voice VLAN вручную.
auto	Укажите, чтобы изучить участников Voice VLAN автоматически.
tag	Укажите, чтобы изучить тегированных участников Voice VLAN.
untag	Укажите, чтобы изучить нетегированных участников Voice VLAN.

По умолчанию

Параметры по умолчанию – **untag** или **auto**.

Режим ввода команды

Interface Configuration Mode.

Использование команды

Используйте данную команду, чтобы настроить автоматическое изучение member-портов Voice VLAN или назначить их вручную.

Если автоматическое изучение включено, порт будет автоматически распознан в качестве member-порта Voice VLAN. В дальнейшем членство будет автоматически удалено согласно времени устаревания. Когда порт работает в автотегированном режиме (**Auto Tag Mode**) и фиксирует

VoIP-устройство через OUI, он автоматически присоединится к Voice VLAN как тегированный порт. Если VoIP-устройство отправляет тегированные пакеты, коммутатор изменит их приоритет. Нетегированные пакеты отправляются в PVID VLAN порта.

Когда порт работает в автонетегированном режиме (**Auto Untag Mode**) и получает информацию о VoIP-устройстве через OUI, он автоматически присоединится к Voice VLAN как нетегированный порт. Если VoIP-устройство отправляет тегированные пакеты, коммутатор изменит их приоритет. Нетегированные пакеты отправляются в Voice VLAN.

Когда коммутатор принимает пакеты LLDP-MED, он проверяет VLAN ID, флаги тега и приоритета, настройкам которых он должен следовать.

Если автоматическое изучение отключено, используйте команду **switchport hybrid vlan** для настройки порта в качестве тегированного или нетегированного member-порта Voice VLAN.

Пример

В данном примере показано, как настроить автотегированный режим (Auto Tag Mode) на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#voice vlan mode auto tag
Switch(config-if)#
```

69.6 voice vlan qos

Данная команда используется для настройки приоритета CoS для входящего трафика Voice VLAN. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

voice vlan qos *COS-VALUE*
no voice vlan qos

Параметры

COS-VALUE	Укажите приоритет Voice VLAN в диапазоне от 0 до 7.

По умолчанию

Значение по умолчанию – 5.

Режим ввода команды

Global Configuration Mode.

Использование команды

Данная команда используется для маркировки CoS VoIP-пакетов, поступающих на порт, на котором включена Voice VLAN. Маркировка CoS позволяет отделить VoIP-трафик от трафика данных по качеству обслуживания.

Пример

В данном примере показано, как настроить приоритет Voice VLAN. Указанное значение – 7.

```
Switch#configure terminal
Switch(config)#voice vlan qos 7
Switch(config)#
```

69.7 show voice vlan

Данная команда используется для отображения настроек Voice VLAN.

show voice vlan [interface [*INTERFACE-ID* **[, | -]]]**
show voice vlan {device | lldp-med device} [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface	(Опционально.) Укажите, чтобы отобразить информацию о портах Voice VLAN.
INTERFACE-ID	(Опционально.) Укажите интерфейс, который необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
device	Укажите, чтобы отобразить VoIP-устройства, информация о которых была получена через OUI.
lldp-med device	Укажите, чтобы отобразить VoIP-устройства, обнаруженные через LLDP-MED.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Использование команды

Данная команда используется для отображения настроек Voice VLAN.

Пример

В данном примере показано, как отобразить глобальные настройки Voice VLAN.

```
Switch#show voice vlan

 Voice VLAN ID         : 1000
 Voice VLAN CoS        : 7
 Aging Time             : 30 minutes
 Member Ports           : eth1/0/1-1/0/5
 Dynamic Member Ports : eth1/0/1-1/0/3
 Voice VLAN OUI:

 OUI Address        Mask               Description
 ---------------   -----------------   ------------
 00-01-E3-00-00-00  FF-FF-FF-00-00-00    Siemens
 00-03-6B-00-00-00  FF-FF-FF-00-00-00    Cisco
 00-09-6E-00-00-00  FF-FF-FF-00-00-00    Avaya
 00-0F-E2-00-00-00  FF-FF-FF-00-00-00    Huawei&3COM
 00-60-B9-00-00-00  FF-FF-FF-00-00-00    NEC&Philips
 00-D0-1E-00-00-00  FF-FF-FF-00-00-00    Pingtel
 00-E0-75-00-00-00  FF-FF-FF-00-00-00    Veritel
 00-E0-BB-00-00-00  FF-FF-FF-00-00-00    3COM
 00-02-03-00-00-00  FF-FF-FF-00-00-00    User1

 Total OUI: 9

Switch#
```

В примере ниже показано, как отобразить информацию о портах Voice VLAN.

```
Switch#show voice vlan interface eth1/0/1-5

Interface     State       Mode
------------  ----------  ------------
eth1/0/1      Enabled     Auto/Tag
eth1/0/2      Enabled     Manual
eth1/0/3      Enabled     Manual
eth1/0/4      Enabled     Auto/Untag
eth1/0/5      Disabled    Manual

Switch#
```

В данном примере показано, как отобразить распознанные VoIP-устройства на интерфейсах Ethernet 1/0/1 и 1/0/2.

```
Switch# show voice vlan device interface eth1/0/1-2

Interface  Device Address     Start Time          Status
---------  ----------------- ----------------  -------
eth1/0/1   00-03-6B-00-00-01  2012-03-19 09:00   Active
eth1/0/1   00-03-6B-00-00-02  2012-03-20 10:09   Aging
eth1/0/1   00-03-6B-00-00-05  2012-03-20 12:04   Active
eth1/0/2   00-03-6B-00-00-0a  2012-03-19 08:11   Aging
eth1/0/2   33-00-61-10-00-11  2012-03-20 06:45   Aging

Total Entries: 5

Switch#
```

В примере ниже показано, как отобразить VoIP-устройства, обнаруженные через LLDP-MED, на интерфейсах Ethernet 1/0/1 и 1/0/2.

```
Switch# show voice vlan lldp-med device interface eth1/0/1-2

Index                 : 1
Interface             : eth1/0/1
Chassis ID Subtype    : MAC Address
Chassis ID            : 00-E0-BB-00-00-11
Port ID Subtype       : Network Address
Port ID               : 172.18.1.1
Create Time           : 2012-03-19 10:00
Remain Time           : 108 Seconds

Index                 : 2
Interface             : eth1/0/2
Chassis ID Subtype    : MAC Address
Chassis ID            : 00-E0-BB-00-00-12
Port ID Subtype       : Network Address
Port ID               : 172.18.1.2
Create Time           : 2012-03-20 11:00
Remain Time           : 105 Seconds

Total Entries: 2

Switch#
```

Приложение A. Записи системного журнала

В таблице ниже перечислены все записи и их соответствующие значения, появляющиеся в системном журнале коммутатора.

802.1X

	Описание записей журнала	Уровень
1	Описание события: ошибка аутентификации 802.1X. Сообщение в журнале: 802.1X authentication fail [due to <reason>] from (Username: <username>, <interface-id>, MAC: <mac-address>). Описание параметров: reason: причина ошибки аутентификации. Возможные причины: (1) Ошибка аутентификации пользователя. (2) Нет ответа от сервера (серверов). (3) Нет настроенных серверов. (4) Нет источников. (5) Время ожидания пользователя истекло. username: пользователь, проходящий аутентификацию. interface-id: номер интерфейса. mac-address: MAC-адрес аутентифицированного устройства.	Критический
2	Описание события: успешная аутентификация 802.1X. Сообщение в журнале: 802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>). Описание параметров: username: пользователь, проходящий аутентификацию. interface-id: имя интерфейса. mac-address: MAC-адрес аутентифицированного устройства.	Информационный

AAA

	Описание записей журнала	Уровень
1	Описание события: глобальное включение/отключение AAA. Сообщение в журнале: AAA is <status>. Описание параметров: status: функция AAA включена или отключена.	Информационный

2	Описание события: успешный вход. Сообщение в журнале: Successful login through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>). Описание параметров: exec-type: типы EXEC: Console, Telnet, SSH, Web, Web (SSL). client-ip: IP-адрес клиента, доступный для IP-протокола. aaa-method: метод аутентификации: none (аутентификация отсутствует), local (использование локальной базы), server (использование сервера). server-ip: IP-адрес AAA-сервера, если методом аутентификации является удаленный сервер. username: имя пользователя аутентификации.	Информационный
3	Описание события: ошибка входа. Сообщение в журнале: Login failed through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>). Описание параметров: exec-type: типы EXEC: Console, Telnet, SSH, Web, Web (SSL). client-ip: IP-адрес клиента, доступный для IP-протокола. aaa-method: метод аутентификации: local (использование локальной базы), server (использование сервера). server-ip: IP-адрес AAA-сервера, если методом аутентификации является удаленный сервер. username: имя пользователя аутентификации.	Предупреждение
4	Описание события: RADIUS назначил атрибуты допустимого VLAN ID. Сообщение в журнале: RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>). Описание параметров: server-ip: IP-адрес RADIUS-сервера. vid: назначенный VLAN ID, авторизованный RADIUS-сервером. interface-id: номер порта аутентифицированного клиента. username: имя пользователя аутентификации.	Информационный

ARP

Описание записей журнала		**Уровень**
1	Описание события: добровольный ARP-запрос (Gratuitous ARP) обнаружил, что другой узел уже использует данный IP-адрес. Сообщение в журнале: Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <port-num>, Interface: <ipif-name>).	Предупреждение

	Описание параметров: ipaddr: заданный IP-адрес, который используется другим узлом. macaddr: заданный MAC-адрес, который используется другим узлом. port-num: номер порта устройства. ipif-name: имя интерфейса коммутатора, из-за IP-адреса которого возник конфликт.	

Auto Image

	Описание записей журнала	Уровень
1	Описание события: обновление ПО через функцию Auto Image выполнено успешно. Сообщение в журнале: The downloaded firmware was successfully executed by DHCP Auto Image update (TFTP Server IP: <ipaddr>). Описание параметров: ipaddr: IP-адрес TFTP-сервера.	Информационный
2	Описание события: обновление ПО через функцию Auto Image выполнить не удалось. Сообщение в журнале: The downloaded firmware was not successfully executed by DHCP AutoImage update (TFTP Server IP: <ipaddr>). Описание параметров: ipaddr: IP-адрес TFTP-сервера.	Информационный

Auto Save Config

	Описание записей журнала	Уровень
1	Описание события: информация о настройках DDP сохраняется автоматически. Сообщение в журнале: CONFIG-6-DDPSAVECONFIG: Configuration automatically saved to flash due to configuring from DDP(Username: <username>, IP: <ipaddr>). Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Информационный

Auto Surveillance VLAN

	Описание записей журнала	Уровень
1	Описание события: обнаружение на интерфейсе нового устройства видеонаблюдения.	Информационный

	Сообщение в журнале: New surveillance device detected (<interface-id>, MAC: <mac-address>). Описание параметров: interface-id: название интерфейса. mac-address: MAC-адрес устройства видеонаблюдения.	
2	Описание события: автоматическое присоединение интерфейса, на котором включена surveillance VLAN, к surveillance VLAN. Сообщение в журнале: <interface-id> add into surveillance VLAN <vid>. Описание параметров: interface-id: название интерфейса. vid: VLAN ID.	Информационный
3	Описание события: выход интерфейса из surveillance VLAN и одновременное отсутствие на этом интерфейсе устройств видеонаблюдения по истечении интервала устаревания (aging). Сообщение в журнале: <interface-id> remove from surveillance VLAN <vid>. Описание параметров: interface-id: название интерфейса. vid: VLAN ID.	Информационный
4	Описание события: добавление IP-камеры в Surveillance VLAN. Сообщение в журнале: ASV: Add IPC (<ipaddr>, MAC:<mac-address>). Описание параметров: ipaddr: IP-адрес IP-камеры. mac-address: MAC-адрес IP-камеры.	Информационный
5	Описание события: удаление IP-камеры из Surveillance VLAN. Сообщение в журнале: ASV: Remove IPC (<ipaddr>, MAC:<mac-address>). Описание параметров: ipaddr: IP-адрес IP-камеры. mac-address: MAC-адрес IP-камеры.	Информационный
6	Описание события: добавление сетевого видеорегистратора в Surveillance VLAN. Сообщение в журнале: ASV: Add NVR (<ipaddr>, MAC:<mac-address>). Описание параметров: ipaddr: IP-адрес сетевого видеорегистратора. mac-address: MAC-адрес сетевого видеорегистратора.	Информационный

7	Описание события: удаление сетевого видеорегистратора из Surveillance VLAN. Сообщение в журнале: ASV: Remove NVR (<ipaddr>, MAC:<mac-address>). Описание параметров: ipaddr: IP-адрес сетевого видеорегистратора. mac-address: MAC-адрес сетевого видеорегистратора.	Информационный
8	Описание события: изменение режима ASV 2.0 при помощи Web-интерфейса. Сообщение в журнале: ASV: Mode change from <mode> to <mode >. Описание параметров: mode: режим ASV 2.0: Standard или Surveillance.	Информационный

Конфигурация/ПО

	Описание записей журнала	**Уровень**
1	Описание события: ПО обновлено успешно. Сообщение в журнале: Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>). Описание параметров: session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента. server-ip: IP-адрес сервера. pathfile: путь и имя файла на сервере.	Информационный
2	Описание события: не удалось обновить ПО. Сообщение в журнале: Firmware upgraded by <session> unsuccessfully (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>). Описание параметров: session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента. server-ip: IP-адрес сервера. pathfile: путь и имя файла на сервере.	Предупреждение

3	Описание события: ПО успешно выгружено. Сообщение в журнале: Firmware uploaded by <session> successfully (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>). Описание параметров: session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента. server-ip: IP-адрес сервера. pathfile: путь и имя файла на сервере.	Информационный
4	Описание события: не удалось выгрузить ПО. Сообщение в журнале: Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>). Описание параметров: session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента. server-ip: IP-адрес сервера pathfile: путь и имя файла на сервере.	Предупреждение
5	Описание события: конфигурация успешно загружена. Сообщение в журнале: Configuration downloaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>). Описание параметров: session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента. server-ip: IP-адрес сервера pathfile: путь и имя файла на сервере.	Информационный

6	Описание события: не удалось загрузить конфигурацию. Сообщение в журнале: Configuration downloaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>). Описание параметров: session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента. server-ip: IP-адрес сервера pathfile: путь и имя файла на сервере.	Предупреждение
7	Описание события: конфигурация успешно выгружена. Сообщение в журнале: Configuration uploaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>). Описание параметров: session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента. server-ip: IP-адрес сервера pathfile: путь и имя файла на сервере.	Информационный
8	Описание события: не удалось выгрузить конфигурацию. Сообщение в журнале: Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>). Описание параметров: session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента. server-ip: IP-адрес сервера. pathfile: путь и имя файла на сервере.	Предупреждение

9	Описание события: конфигурация сохранена на флэш-память через консоль. Сообщение в журнале: Configuration saved to flash by console (Username: <username>). Описание параметров: username: имя текущего пользователя.	Информационный
10	Описание события: конфигурация сохранена на флэш-память удаленно. Сообщение в журнале: Configuration saved to flash (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Информационный
11	Описание события: сообщение успешно выгружено. Сообщение в журнале: Log message uploaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>]). Описание параметров: session: сессия пользователя. username: имя текущего пользователя ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента.	Информационный
12	Описание события: не удалось выгрузить сообщение. Сообщение в журнале: Log message uploaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>]). Описание параметров: session: сессия пользователя. username: имя текущего пользователя ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента.	Предупреждение

13	Описание события: не удалось загрузить файлы неизвестного типа. Сообщение в журнале: Downloaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>). Описание параметров: session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента. server-ip: IP-адрес сервера pathfile: путь и имя файла на сервере.	Предупреждение

Примечание:

- Сессия пользователя указывает на доступ через Console, Web, SNMP, Telnet или SSH.
- Если обновление конфигурации/ПО выполняется через консоль, информация об IP- и MAC-адресах в журнале указываться не будет.

DAD

Описание записей журнала		**Уровень**
1	Описание события: событие о дублированном адресе во время процесса DAD будет добавлено в журнал, после того как DUT получит сообщение Neighbor Solicitation (NS). Сообщение в журнале: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Solicitation Messages. Описание параметров: ipv6address: IPv6-адрес сообщений Neighbor Solicitation. interface-id: имя интерфейса.	Предупреждение
2	Описание события: событие о дублированном адресе во время процесса DAD будет добавлено в журнал, после того как DUT получит сообщение Neighbor Advertisement (NA). Сообщение в журнале: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Advertisement Messages. Описание параметров: ipv6address: IPv6-адрес сообщений Neighbor Advertisement. interface-id: имя интерфейса.	Предупреждение

DAI

	Описание записей журнала	Уровень
1	Описание события: обнаружен запрещенный ARP-пакет. Сообщение в журнале: Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>). Описание параметров: type: тип ARP-пакета (request или response). ip-address: IP-адрес. mac-address: MAC-адрес. vlan-id: VLAN ID. interface-id: имя интерфейса.	Предупреждение
2	Описание события: обнаружен допустимый ARP-пакет. Сообщение в журнале: Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>). Описание параметров: type: тип ARP-пакета (request или response). ip-address: IP-адрес. mac-address: MAC-адрес. vlan-id: VLAN ID. interface-id: имя интерфейса.	Информационный

DHCPv6 Client

	Описание записей журнала	Уровень
1	Описание события: состояние DHCPv6-клиента на указанном интерфейсе изменено администратором. Сообщение в журнале: DHCPv6 client on interface <ipif-name> changed state to [enabled | disabled]. Описание параметров: ipif-name: имя интерфейса DHCPv6-клиента.	Информационный
2	Описание события: DHCPv6-клиент получил IPv6-адрес от сервера DHCPv6. Сообщение в журнале: DHCPv6 client obtains an ipv6 address <ipv6address> on interface <ipif-name>. Описание параметров: ipv6address: IPv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса DHCPv6-клиента.	Информационный

3	Описание события: IPv6-адрес, полученный от сервера DHCPv6, обновляется. Сообщение в журнале: The IPv6 address <ipv6address> on interface <ipif-name> starts renewing. Описание параметров: ipv6address: IPv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса DHCPv6-клиента.	Информационный
4	Описание события: IPv6-адрес, полученный от сервера DHCPv6, успешно обновлен. Сообщение в журнале: The IPv6 address <ipv6address> on interface <ipif-name> renews success. Описание параметров: ipv6address: IPv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса DHCPv6-клиента.	Информационный
5	Описание события: выполняется повторная привязка IPv6-адреса, полученного от сервера DHCPv6. Сообщение в журнале: The IPv6 address <ipv6address> on interface <ipif-name> starts rebinding. Описание параметров: ipv6address: IPv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса DHCPv6-клиента.	Информационный
6	Описание события: повторная привязка IPv6-адреса, полученного от сервера DHCPv6, выполнена успешно. Сообщение в журнале: The IPv6 address <ipv6address> on interface <ipif-name> rebinds success. Описание параметров: ipv6address: IPv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса DHCPv6-клиента.	Информационный
7	Описание события: IPv6-адрес, полученный от сервера DHCPv6, удален. Сообщение в журнале: The IPv6 address <ipv6address> on interface <ipif-name> was deleted. Описание параметров: ipv6address: IPv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса DHCPv6-клиента.	Информационный

DHCPv6 Relay

	Описание записей журнала	Уровень
1	Описание события: состояние DHCPv6-клиента на указанном интерфейсе изменено администратором. Сообщение в журнале: DHCPv6 relay on interface <ipif-name> changed state to [enabled | disabled] Описание параметров: <ipif-name>: имя интерфейса DHCPv6-клиента.	Информационный

DNS Resolver

	Описание записей журнала	Уровень
1	Описание события: добавлено дублирующееся доменное имя, в результате чего запись DNS будет удалена из динамического кэша. Сообщение в журнале: Duplicate Domain name case name: <domain-name>, static IP: <ipaddr>, dynamic IP:<ipaddr>. Описание параметров: domain-name: доменное имя. ipaddr: статический / динамический IP-адрес.	Информационный

DoS Prevention

	Описание записей журнала	Уровень
1	Описание события: обнаружена DoS-атака. Сообщение в журнале: <dos-type> is dropped from (IP: <ip-address> Port <interface-id>). Описание параметров: dos-type: тип DoS-атаки. ip-address: IP-адрес. interface-id: имя интерфейса.	Уведомление

Interface

	Описание записей журнала	Уровень
1	Описание события: соединение на порту прервано. Сообщение в журнале: Port <port-type>< interface-id> link down Описание параметров: port-type: тип порта. interface-id: имя интерфейса.	Информационный

2	Описание события: соединение на порту установлено. Сообщение в журнале: Port <port-type>< interface-id> link up, <link-speed> Описание параметров: port-type: тип порта. interface-id: имя интерфейса. link-speed: скорость канала порта.	Информационный

IP Source Guard

	Описание записей журнала	**Уровень**
1	Описание события: ошибка создания записи DHCP Snooping в таблице IPSG из-за отсутствия ресурсов аппаратных правил. Сообщение в журнале: Failed to set IPSG entry due to no hardware rule resource. (IP: <ipaddr>, MAC: <macaddr>, VID: <vlanid>, Interface <interface-id>). Описание параметров: ipaddr: IP-адрес. macaddr: MAC-адрес. vlanid: VLAN ID interface-id: имя интерфейса.	Предупреждение

IPv6 Source Guard

	Описание записей журнала	**Уровень**
1	Описание события: ошибка создания записи IPv6 Snooping в таблице IPv6SG из-за отсутствия ресурсов аппаратных правил. Сообщение в журнале: Failed to set IPv6SG entry due to no hardware rule resource. (IP: <ipaddr>, MAC: <macaddr>, VID: <vlan-id>, Interface <interface-id>). Описание параметров: ipaddr: IPv6-адрес записи IPv6 Snooping. macaddr: MAC-адрес записи IPv6 Snooping. vlan-id: VID записи IPv6 Snooping. interface-id: интерфейс записи IPv6 Snooping.	Предупреждение

LACP

	Описание записей журнала	**Уровень**
1	Описание события: группа агрегирования (Link Aggregation) включена. Сообщение в журнале: Link Aggregation Group <group-id> link up. Описание параметров: group-id: ID включенной группы агрегирования.	Информационный

2	Описание события: группа агрегирования (Link Aggregation) отключена. Сообщение в журнале: Link Aggregation Group <group-id> link down. Описание параметров: group-id: ID включенной группы агрегирования.	Информационный
3	Описание события: member-порт присоединился к группе агрегирования. Сообщение в журнале: <ifname> attach to Link Aggregation Group <group-id>. Описание параметров: ifname: имя интерфейса порта, который был присоединен к группе агрегирования. group-id: ID группы агрегирования, к которой был присоединен порт.	Информационный
4	Описание события: member-порт покинул группу агрегирования. Сообщение в журнале: <ifname> detach from Link Aggregation Group <group-id>. Описание параметров: ifname: имя интерфейса порта, который покинул группу агрегирования. group-id: ID группы агрегирования, которую покинул порт.	Информационный

LBD

Описание записей журнала		**Уровень**
1	Описание события: на интерфейсе обнаружена петля. Сообщение в журнале: <interface-id> LBD loop occurred. Описание параметров: interface-id: интерфейс, на котором обнаружена петля.	Критический
2	Описание события: на интерфейсе обнаружена петля в VLAN. Сообщение в журнале: <interface-id> VLAN <vlan-id> LBD loop occurred. Описание параметров: interface-id: интерфейс, на котором обнаружена петля. vlan-id: VLAN, на которой обнаружена петля.	Критический
3	Описание события: на интерфейсе обнаружена петля. Сообщение в журнале: <interface-id> LBD loop recovered. Описание параметров: interface-id: интерфейс, на котором обнаружена петля.	Критический
4	Описание события: на интерфейсе обнаружена петля в VLAN. Сообщение в журнале: <interface-id> VLAN <vlan-id> LBD loop recovered. Описание параметров: interface-id: интерфейс, на котором обнаружена петля. vlan-id: VLAN, на которой обнаружена петля.	Критический
5	Описание события: число VLAN, на которых была обнаружена петля, превысило указанное число. Сообщение в журнале: Loop VLAN numbers overflow.	Критический

LLDP/LLDP-MED

	Описание записей журнала	Уровень
1	Описание события: обнаружено изменение топологии LLDP-MED. Сообщение в журнале: LLDP-MED topology change detected (on port <portNum>. chassis ID: <chassisType>, <chassisID>, port ID: <portType>, <portID>, device class: <deviceClass>). Описание параметров: portNum: номер порта. chassisType: список подтипов ID шасси: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: ID шасси. portType: список подтипов ID порта: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: ID порта. deviceClass: тип устройства LLDP-MED.	Уведомление
2	Описание события: обнаружен конфликт типа устройства LLDP-MED. Сообщение в журнале: Conflict LLDP-MED device type detected (on port <portNum>, chassis ID: <chassisType>, <chassisID>, port ID: <portType>, <portID>, device class: <deviceClass>). Описание параметров: portNum: номер порта. chassisType: список подтипов ID шасси: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: ID шасси. portType: список подтипов ID порта: 1. interfaceAlias(1) 2. portComponent(2)	Уведомление

	3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: ID порта. deviceClass: тип устройства LLDP-MED.	
3	Описание события: обнаружен несовместимый набор TLV LLDP-MED. Сообщение в журнале: Incompatible LLDP-MED TLV set detected (on port <portNum>, chassis ID: <chassisType>, <chassisID>, port ID: <portType>, <portID>, device class: <deviceClass>). Описание параметров: portNum: номер порта. chassisType: список подтипов ID шасси: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: ID шасси. portType: список подтипов ID порта: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: ID порта. deviceClass: тип устройства LLDP-MED.	Уведомление

Login/Logout CLI

	Описание записей журнала	**Уровень**
1	Описание события: успешный вход через консоль. Сообщение в журнале: Successful login through Console (Username: <username>). Описание параметров: username: имя текущего пользователя.	Информационный
2	Описание события: не удалось выполнить вход через консоль. Сообщение в журнале: Login failed through Console (Username: <username>). Описание параметров: username: имя текущего пользователя.	Предупреждение

3	Описание события: время сессии в консоли истекло. Сообщение в журнале: Console session timed out (Username: <username>). Описание параметров: username: имя текущего пользователя.	Информационный
4	Описание события: выполнен выход через консоль. Сообщение в журнале: Logout through Console (Username: <username>). Описание параметров: username: имя текущего пользователя.	Информационный
5	Описание события: успешный вход через Telnet. Сообщение в журнале: Successful login through Telnet (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Информационный
6	Описание события: не удалось выполнить вход через Telnet. Сообщение в журнале: Login failed through Telnet (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Предупреждение
7	Описание события: время сессии Telnet истекло. Сообщение в журнале: Telnet session timed out (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Информационный
8	Описание события: выполнен выход через Telnet. Сообщение в журнале: Logout through Telnet (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Информационный
9	Описание события: успешный вход через SSH. Сообщение в журнале: Successful login through SSH (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Информационный

10	Описание события: не удалось выполнить вход через SSH. Сообщение в журнале: Login failed through SSH (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Критический
11	Описание события: время сессии SSH истекло. Сообщение в журнале: SSH session timed out (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Информационный
12	Описание события: выполнен выход через SSH. Сообщение в журнале: Logout through SSH (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Информационный

MSTP Debug Enhancement

	Описание записей журнала	**Уровень**
1	Описание события: Spanning Tree Protocol включен. Сообщение в журнале: Spanning Tree Protocol is enabled.	Информационный
2	Описание события: Spanning Tree Protocol отключен. Сообщение в журнале: Spanning Tree Protocol is disabled.	Информационный
3	Описание события: изменилась топология экземпляра MSTP. Сообщение в журнале: Topology changed (Instance: <instance-id>,<interface-id>, MAC:<macaddr>). Описание параметров: instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST. interface-id: номер порта, обнаружевшего или получившего информацию об изменении топологии. macaddr: система MAC-адреса моста.	Уведомление
4	Описание события: выбран новый корневой мост экземпляра MSTP. Сообщение в журнале: [CIST | CIST Region | MSTI Region] New Root bridge selected ([Instance: <instance-id>] MAC: <macaddr> Priority:<priority>). Описание параметров: instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST. macaddr: система MAC-адресов моста. priority: значение приоритета моста должно быть кратным 4096.	Информационный

5	Описание события: выбран новый корневй мост экземпляра MSTP. Сообщение в журнале: New root port selected (Instance:<instance-id>, <interface-id>). Описание параметров: instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST. interface-id: номер порта, обнаружевшего или получившего информацию об изменении топологии.	Уведомление
6	Описание события: изменился статус порта экземпляра MSTP. Сообщение в журнале: Spanning Tree port status change (Instance:<instance-id>, <interface-id>) <old-status> -> <new-status>. Описание параметров: instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST. interface-id: номер порта, обнаружевшего или получившего информацию об изменении топологии. old-status: предыдущий статус порта (Disable, Discarding, Learning или Forwarding). new-status: новый статус порта (Disable, Discarding, Learning или Forwarding).	Уведомление
7	Описание события: изменилась роль порта экземпляра MSTP. Сообщение в журнале: Spanning Tree port role change (Instance:<instance-id>, <interface-id>) <old-role> -> <new-role>. Описание параметров: instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST. interface-id: номер порта, обнаружевшего или получившего информацию об изменении топологии. old-role: предыдущая роль STP (DisablePort, AlternatePort, BackupPort, RootPort, DesignatedPort, NonstpPort или MasterPort). new-role: новая роль STP (DisablePort, AlternatePort, BackupPort, RootPort, DesignatedPort, NonstpPort или MasterPort).	Информационный
8	Описание события: создан экземпляр MSTP. Сообщение в журнале: Spanning Tree instance created (Instance:<instance-id>). Описание параметров: instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST.	Информационный
9	Описание события: удален экземпляр MSTP. Сообщение в журнале: Spanning Tree instance deleted (Instance:<instance-id>). Описание параметров: instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST.	Информационный

10	Описание события: изменена версия STP. Сообщение в журнале: Spanning Tree version change (new version:<new-version>). Описание параметров: new-version: версия STP.	Информационный
11	Описание события: имя конфигурации и revision level изменились в MST Configuration Identification. Сообщение в журнале: Spanning Tree MST configuration ID name and revision level change (name:<name>, revision level <revision-level>). Описание параметров: name: имя конкретного региона MST. revision-level: коммутаторы с одинаковым именем, но разными revision level считаются членами разных регионов MST.	Информационный
12	Описание события: привязка VLAN к экземпляру MST. Сообщение в журнале: Spanning Tree MST configuration ID VLAN mapping table change (instance: <instance-id> add vlan <startvlanid> [- <endvlanid>]). Parameters Description: instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST. startvlanid: начальный vid для добавления диапазона vlan. endvlanid: конечный vid для добавления диапазона vlan.	Информационный
13	Описание события: удаление VLAN из экземпляра MST. Сообщение в журнале: Spanning Tree MST configuration ID VLAN mapping table change (instance: <instance-id> delete vlan <startvlanid> [- <endvlanid>]). Parameters Description: instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST. startvlanid: начальный vid для удаления диапазона vlan. endvlanid: конечный vid для удаления диапазона vlan.	Информационный
14	Описание события: присвоена роль альтернативного порта (Alternate Port) из-за Root Guard. Сообщение в журнале: Spanning Tree port role change (Instance:<instance-id>, <interface-id>) to alternate port due to the guard root Parameters Description: instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST. interface-id: номер порта, обнаружевшего событие.	Информационный

Peripheral

Описание записей журнала		**Уровень**
1	Описание события: вентилятор восстановлен. Сообщение в журнале: <fan-descr> back to normal. Описание параметров: fan-descr: ID и положение вентилятора.	Критический

2	Описание события: вентилятор вышел из строя. Сообщение в журнале: <fan-descr> failed. Описание параметров: fan-descr: ID и положение вентилятора.	Критический
3	Описание события: датчик температуры показывает критическое значение. Сообщение в журнале: <thermal-sensor-descr> detects abnormal temperature <degree>. Описание параметров: thermal-sensor-descr: ID и положение датчика. degree: текущая температура.	Критический
4	Описание события: возврат температуры к нормальному значению. Сообщение в журнале: <thermal-sensor-descr> temperature back to normal. Описание параметров: thermal-sensor-descr: ID и положение датчика.	Критический
5	Описание события: нажата кнопка возврата к заводским настройкам. Сообщение в журнале: Factory reset button pressed	Критический

Port Security

	Описание записей журнала	**Уровень**
1	Описание события: нарушение безопасности порта, вызванное MAC-адресом. Сообщение в журнале: MAC address <macaddr> causes port security violation on <interface-id>. Описание параметров: macaddr: недопустимый MAC-адрес. interface-id: имя интерфейса.	Предупреждение
2	Описание события: превышено максимальное количество адресов в системе. Сообщение в журнале: Limit on system entry number has been exceeded	Предупреждение

Safeguard

	Описание записей журнала	**Уровень**
1	Описание события: коммутатор перешел в режим высокой загрузки. Сообщение в журнале: Safeguard Engine enters EXHAUSTED mode.	Предупреждение
2	Описание события: коммутатор перешел в нормальный режим. Сообщение в журнале: Safeguard Engine enters NORMAL mode.	Информационный

SNMP

Описание записей журнала	**Уровень**

1	Описание события: получен запрос SNMP с неверной строкой сообщества. Сообщение в журнале: SNMP request received from <ipaddr> with invalid community string. Описание параметров: ipaddr: IP-адрес.	Информационный

SSH

	Описание записей журнала	**Уровень**
1	Описание события: SSH-сервер включен. Сообщение в журнале: SSH server is enabled.	Информационный
2	Описание события: SSH-сервер отключен. Сообщение в журнале: SSH server is disabled.	Информационный

Storm Control

	Описание записей журнала	**Уровень**
1	Описание события: возникновение шторма. Сообщение в журнале: <Broadcast | Multicast | Unicast> storm is occurring on <interface-id>. Описание параметров: Broadcast: шторм, возникший из-за широковещательных пакетов (DA = FF:FF:FF:FF:FF:FF). Multicast: шторм, возникший из-за многоадресных пакетов, включая известные и неизвестные пакеты 2 уровня, пакеты с известным и неизвестным IP. Unicast: шторм, возникший из-за одноадресных пакетов, включая известные и неизвестные пакеты. interface-id: ID интерфейса, на котором возник шторм.	Предупреждение
2	Описание события: шторм устранен. Сообщение в журнале: <Broadcast | Multicast | Unicast> storm is cleared on <interface-id> Описание параметров: Broadcast: устранен шторм широковещательных пакетов (Broadcast Storm). Multicast: устранен шторм многоадресных пакетов (Multicast Storm). Unicast: устранен шторм одноадресных пакетов, включая известные и неизвестные пакеты (Unicast Storm). interface-id: ID интерфейса, на котором шторм устранен.	Информационный

3	Описание события: соединение на порту прервано из-за возникновение шторма. Сообщение в журнале: <interface-id> is currently shut down due to the <Broadcast | Multicast | Unicast> storm. Описание параметров: interface-id: ID интерфейса, находящегося в состоянии error-disabled из-за шторма. Broadcast: интерфейс отключен из-за шторма широковещательных пакетов. Multicast: интерфейс отключен из-за шторма многоадресных пакетов. Unicast: интерфейс отключен из-за шторма одноадресных пакетов, включая известные и неизвестные пакеты.	Предупреждение

System

Описание записей журнала		**Уровень**
1	Описание события: сообщение генерируется при горячем старте. Сообщение в журнале: System warm start.	Критический
2	Описание события: сообщение генерируется при холодном старте. Сообщение в журнале: System cold start.	Критический
3	Описание события: сообщение генерируется при старте системы. Сообщение в журнале: System started up.	Критический

Telnet

Описание записей журнала		**Уровень**
1	Описание события: успешный вход через Telnet. Сообщение в журнале: Successful login through Telnet (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя Telnet-клиента. ipaddr: IP-адрес Telnet-клиента.	Информационный
2	Описание события: не удалось выполнить вход через Telnet. Сообщение в журнале: Login failed through Telnet (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя Telnet-клиента. ipaddr: IP-адрес Telnet-клиента.	Предупреждение
3	Описание события: выполнен выход через Telnet. Сообщение в журнале: Logout through Telnet (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя Telnet-клиента. ipaddr: IP-адрес Telnet-клиента.	Информационный

4	Описание события: время сессии Telnet истекло. Сообщение в журнале: Telnet session timed out (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя Telnet-клиента. ipaddr: IP-адрес Telnet-клиента.	Информационный

Voice VLAN

	Описание записей журнала	Уровень
1	Описание события: на интерфейсе обнаружено новое устройство VoIP. Сообщение в журнале: New voice device detected (<interface-id>, MAC: <mac-address>). Описание параметров: interface-id: название интерфейса. mac-address: MAC-адрес устройства VoIP.	Информационный
2	Описание события: интерфейс, который находится в режиме auto voice VLAN, присоединяется к voice VLAN. Сообщение в журнале: <interface-id> add into voice VLAN <vid>. Описание параметров: interface-id: название интерфейса. vid: VLAN ID.	Информационный
3	Описание события: сообщение появляется, когда интерфейс покидает voice VLAN, и при этом на интерфейсе не обнаруживаются устройства VoIP за интервал устаревания (aging). Сообщение в журнале: <interface-id> remove from voice VLAN <vid>. Описание параметров: interface-id: название интерфейса. vid: VLAN ID.	Информационный

Web

	Описание записей журнала	Уровень
1	Описание события: успешный вход через Web. Сообщение в журнале: Successful login through Web (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя HTTP-клиента. ipaddr: IP-адрес HTTP-клиента.	Информационный

2	Описание события: не удалось войти через Web. Сообщение в журнале: Login failed through Web (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя HTTP-клиента. ipaddr: IP-адрес HTTP-клиента.	Предупреждение
3	Описание события: время сессии Web истекло. Сообщение в журнале: Web session timed out (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя HTTP-клиента. ipaddr: IP-адрес HTTP-клиента.	Информационный
4	Описание события: выполнен выход через Web. Сообщение в журнале: Logout through Web (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя HTTP-клиента. ipaddr: IP-адрес HTTP-клиента.	Информационный
5	Описание события: успешный вход через Web (SSL). Сообщение в журнале: Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя пользователя, используемое для входа на SSL-сервер. ipaddr: IP-адрес SSL-клиента.	Информационный
6	Описание события: не удалось войти через Web (SSL). Сообщение в журнале: Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя пользователя, используемое для входа на SSL-сервер. ipaddr: IP-адрес SSL-клиента.	Предупреждение
7	Описание события: время сессии Web (SSL) истекло. Сообщение в журнале: Web (SSL) session timed out (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя пользователя, используемое для входа на SSL-сервер. ipaddr: IP-адрес SSL-клиента.	Информационный
8	Описание события: выполнен выход через Web (SSL). Сообщение в журнале: Logout through Web (SSL) (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя пользователя, используемое для входа на SSL-сервер. ipaddr: IP-адрес SSL-клиента.	Информационный

Приложение B. Записи trap-сообщений

Таблица ниже содержит записи trap-сообщений и их соответствующие значения, встречающиеся на коммутаторе.

802.1X

Сообщение trap		Описание	OID
1	dDot1xExtLoggedSuccess	Узел прошел аутентификацию IEEE 802.1X. Вариабельные привязки: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName	1.3.6.1.4.1.17 1.14.30.0.1
2	dDot1xExtLoggedFail	Узел не прошел аутентификацию IEEE 802.1X. Вариабельные привязки: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName (5) dDot1xExtNotifyFailReason	1.3.6.1.4.1.17 1.14.30.0.2

Authentication Fail

Сообщение trap		Описание	OID
1	authenticationFailure	SNMPv2-устройство в роли агента получило сообщение протокола, которое не аутентифицировано должным образом. Данное trap-сообщение генерируется всеми реализациями SNMPv2 и будет отправлено, только если параметр snmpEnableAuthenTraps включен.	1.3.6.1.6.3.1.1 .5.5

DHCP Server Screen Prevention

Сообщение trap		Описание	OID
1	dDhcpFilterAttackDetected	Включена функция DHCP Server Screen, коммутатор получил пакет ложного DHCP-сервера. Вариабельные привязки: (1) dDhcpFilterLogBufServerIpAddr (2) dDhcpFilterLogBufClientMacAddr (3) dDhcpFilterLogBufferVlanId (4) dDhcpFilterLogBufferOccurTime	1.3.6.1.4.1.17 1.14.133.0.1

DoS Prevention

Сообщение trap		Описание	OID
1	dDosPreveAttackDetectedPacket	Обнаружена DoS-атака. Вариабельные привязки: (1) dDoSPrevCtrlAttackType	1.3.6.1.4.1.17 1.14.59.0.2

		(2) dDosPrevNotiInfoDropIpAddr (3) dDosPrevNotiInfoDropPortNumber	

ErrDisable

	Сообщение trap	Описание	OID
1	dErrDisNotifyPortDisabledAssert	Порт перешел в состояние Error-Disabled. Вариабельные привязки: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.17 1.14.45.0.1
2	dErrDisNotifyPortDisabledClear	Порт возвращается в исходное состояние по истечении определенного интервала времени. Вариабельные привязки: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.17 1.14.45.0.2

General Management

	Сообщение trap	Описание	OID
1	dGenMgmtLoginFail	Ошибка авторизации на коммутаторе. Вариабельные привязки: (1) dGenMgmtNotifyInfoLoginType (2) dGenMgmtNotifyInfoUserName	1.3.6.1.4.1.17 1.14.165.0.1

Gratuitous ARP

	Сообщение trap	Описание	OID
1	agentGratuitousARPTrap	Обнаружен конфликт IP-адреса. Вариабельные привязки: (1) ipaddr (2) macaddr (3) portNumber (4) agentGratuitousARPInterfaceName	1.3.6.1.4.1.17 1.14.75.0.1

IP-MAC-Port Binding

	Сообщение trap	Описание	OID
1	dImpbViolationTrap	Обнаружен недопустимый адрес привязки IP-MAC-Port Binding. Вариабельные привязки: (1) ifIndex (2) dImpbViolationIpAddrType (3) dImpbViolationIpAddress (4) dImpbViolationMacAddress (5) dImpbViolationVlan	1.3.6.1.4.1.17 1.14.22.0.1

LACP

Сообщение trap	Описание	OID

1	linkUp	SNMP-устройство в роли агента обнаружило, что один из каналов связи перешел из состояния «down» в какое-то другое состояние (за исключением состояния notPresent). Текущее состояние указано в привязке ifOperStatus. Вариабельные привязки: (1) ifIndex, (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
2	linkDown	SNMP-устройство в роли агента обнаружило, что один из каналов связи перешел в состояние «down» из какого-то другого состояния (за исключением состояния notPresent). Предыдущее состояние указано в привязке ifOperStatus. Вариабельные привязки: (1) ifIndex, (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3

LBD

Сообщение trap		**Описание**	**OID**
1	dLbdLoopOccurred	Обнаружена петля. Вариабельные привязки: (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.17 1.14.46.0.1
2	dLbdLoopRestart	Порт возвращается в исходное состояние по истечении определенного интервала времени. Вариабельные привязки: (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.17 1.14.46.0.2
3	dLbdVlanLoopOccurred	Порт перешел в состояние возникновения петли в VID. Вариабельные привязки: (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.17 1.14.46.0.3
4	dLbdVlanLoopRestart	Порт в VID возвращается в исходное состояние по истечению определенного интервала времени. Вариабельные привязки: (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.17 1.14.46.0.4

LLDP/LLDP-MED

Сообщение trap		**Описание**	**OID**
1	lldpRemTablesChange	Значение lldpStatsRemTableLastChangeTime изменилось. Вариабельные привязки: (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes	1.0.8802.1.1.2 .0.0.1

		(3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	
2	lldpXMedTopologyChangeDetected	Обнаружено изменение в топологии: к порту было подключено новое устройство, удаленное устройство было отключено или было отключено с дальнейшим подключением к другому порту. Вариабельные привязки: (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass	1.0.8802.1.1.2.1.5.4795.0.1

MAC Notification

	Сообщение trap	Описание	OID
1	swL2macNotification	Изменение MAC-адресов в таблице коммутации. Вариабельные привязки: (1) swL2macNotifyInfo	1.3.6.1.4.1.171.14.3.0.1
2	dL2FdbMacNotificationWithVID	Изменение MAC-адресов в таблице коммутации с VLAN ID. Вариабельные привязки: (1) dL2FdbMacChangeNotifyInfoWithVID	1.3.6.1.4.1.171.14.3.0.2

MSTP

	Сообщение trap	Описание	OID
1	newRoot	Новый корень Spanning Tree. Trap-собщение будет отправлено мостом сразу же после его назначения в качестве нового корня. По истечении таймера (Topology Change Timer) мост немедленно будет назначен корнем. Отправка данного trap-собщения является опциональной.	1.3.6.1.2.1.17.0.1
2	topologyChange	Мост отправляет trap-собщение, когда какой-то из его настроенных портов переходит из состояния learning в состояние forwarding или из состояния forwarding в состояние blocking. Данное trap-собщение не отправляется повторно. Отправка данного trap-сообщения является опциональной.	1.3.6.1.2.1.17.0.2

Peripheral

	Сообщение trap	Описание	OID
1	dEntityExtFanStatusChg	Вентилятор вышел из строя. Данное trap-сообщение отправляется Commander Switch. Уведомление dEntityExtEnvFanStatus может быть «fault», а при восстановлении вентилятора – «ok». Вариабельные привязки: (1) dEntityExtEnvFanUnitId	1.3.6.1.4.1.171.14.5.0.1

		(2) dEntityExtEnvFanIndex (3) dEntityExtEnvFanStatus	
2	dEntityExtThermalStatusChg	Датчик температуры показывает критическое значение. Данное trap-сообщение отправляется Commander Switch. Уведомление dEntityExtEnvTempStatus может быть «abnormal», а при возвращении температуры к нормальному значению – «ok». Вариабельные привязки: (1) dEntityExtEnvTempUnitId (2) dEntityExtEnvTempIndex (3) dEntityExtEnvTempStatus	1.3.6.1.4.1.17 1.14.5.0.2

Port

Сообщение trap		Описание	OID
1	linkUp	Соединение на порту установлено. Вариабельные привязки: (1) ifIndex, (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1 .5.4
2	linkDown	Соединение на порту прервано. Вариабельные привязки: (1) ifIndex (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1 .5.3

Port Security

Сообщение trap		Описание	OID
1	dPortSecMacAddrViolation	Trap-сообщения будут отправлены при обнаружении недопустимых MAC-адресов. Вариабельные привязки: (1) ifIndex (2) dPortSecIfCurrentStatus (3) dPortSecIfViolationMacAddress	1.3.6.1.4.1.17 1.14.8.0.1

RMON

Сообщение trap		Описание	OID
1	risingAlarm	Запись уровня alarm превысила заданный верхний порог. Вариабельные привязки: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16. 0.1

2	fallingAlarm	Запись уровня alarm снизилась до заданного нижнего порога. Вариабельные привязки: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16.0.2

Safeguard

Сообщение trap		Описание	OID
1	dSafeguardChgToExhausted	Нормальный режим работы системы изменился на режим высокой загрузки. Вариабельные привязки: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.171.14.19.1.1.0.1
2	dSafeguardChgToNormal	Режим высокой загрузки системы изменился на нормальный режим. Вариабельные привязки: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.171.14.19.1.1.0.2

Start

Сообщение trap		Описание	OID
1	coldStart	Повторная инициализация SNMPv2-устройства в роли агента и возможное изменение его настроек.	1.3.6.1.6.3.1.1.5.1
2	warmStart	Повторная инициализация SNMPv2-устройства в роли агента с неизмененной конфигурацией.	1.3.6.1.6.3.1.1.5.2

Storm Control

Сообщение trap		Описание	OID
1	dStormCtrlOccurred	Данное trap-сообщение будет отправлено, если параметр dStormCtrlNotifyEnable имеет значение «stormOccurred» или «both», а также при возникновении шторма. Вариабельные привязки: (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171.14.25.0.1
2	dStormCtrlStormCleared	Данное trap-сообщение будет отправлено, если параметр dStormCtrlNotifyEnable имеет значение «stormCleared» или «both», а также при устранении шторма. Вариабельные привязки: (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171.14.25.0.2

System File

Сообщение trap		Описание	OID
1	dsfUploadImage	Пользователь успешно выгрузил файл образа.	1.3.6.1.4.1.17 1.14.14.0.1
2	dsfDownloadImage	Пользователь успешно загрузил файл образа.	1.3.6.1.4.1.17 1.14.14.0.2
3	dsfUploadCfg	Пользователь успешно выгрузил конфигурационный файл.	1.3.6.1.4.1.17 1.14.14.0.3
4	dsfDownloadCfg	Пользователь успешно загрузил конфигурационный файл.	1.3.6.1.4.1.17 1.14.14.0.4
5	dsfSaveCfg	Пользователь успешно сохранил конфигурационный файл.	1.3.6.1.4.1.17 1.14.14.0.5

Приложение C. Назначение атрибутов RADIUS

На коммутаторе назначение атрибутов RADIUS используется в модуле 802.1X.
Ниже представлены следующие атрибуты RADIUS:

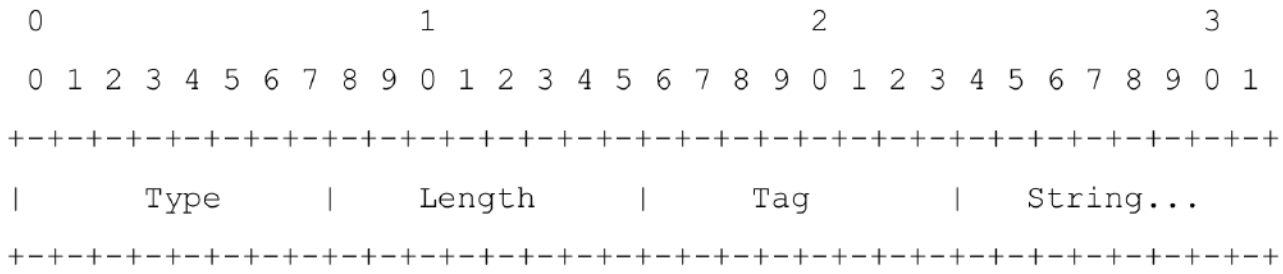
- VLAN

Для того чтобы RADIUS-сервер назначил **VLAN**, необходимо сконфигурировать соответствующие параметры на сервере. Для назначения VLAN RFC 3580 определяет следующие атрибуты в пакетах RADIUS.

Параметры для VLAN:

RADIUS Tunnel Attribute	Описание	Значение	Использование
Tunnel-Type	Этот атрибут указывает туннельный протокол, который нужно использовать в качестве инициатора или терминатора туннеля	13 (VLAN)	Обязательно
Tunnel-Medium-Type	Атрибут указывает используемую среду передачи	6 (802)	Обязательно
Tunnel-Private-Group-ID	Атрибут указывает групповой ID для определенной туннельной сессии	Строка (VID)	Обязательно

Ниже показана краткая информация о формате атрибута Tunnel-Private-Group-ID:



В таблице ниже приведено описание поля Tag, которое отличается от RFC 2868:

Значение поля Tag	Формат строки поля
0x01	Название VLAN (ASCII)
0x02	VLAN ID (ASCII)
Другие (0x00, 0x03 ~ 0x1F, >0x1F)	При получении строки настройки VLAN коммутатор сначала будет проверять все существующие VLAN ID и выберет подходящий, который станет идентификатором данной VLAN. Если подходящий VLAN ID отсутствует, коммутатор будет проверять доступные имена VLAN.

Примечание: поле тега больше 0x1F распознается как первый октет следующего поля.

Если пользователь сконфигурировал атрибут VLAN на RADIUS-сервере (например, VID 3) и аутентификация 802.1X прошла успешно, порт будет назначен в VLAN 3. Однако если пользователь

не сконфигурировал атрибуты VLAN, порт, который не является членом Guest VLAN, останется в текущей VLAN аутентификации, а порт, являющийся членом Guest VLAN, будет назначен в исходную VLAN.

Приложение D. Поддержка атрибутов IETF RADIUS

Для атрибутов RADIUS существуют определенные параметры аутентификации, авторизации и конфигурации для запросов и ответов. В данном разделе приведен список атрибутов RADIUS, которые в данный момент поддерживает коммутатор.

Атрибуты RADIUS поддерживаются стандартом IETF и Vendor-Specific Attribute (VSA). VSA позволяет призводителям создавать собственные дополнительные атрибуты RADIUS. Для подробной информации о VSA D-Link обратитесь к **Приложению «Назначение атрибутов RADIUS»**.

Атрибуты RADIUS стандарта IETF определены в RFC 2865 Remote Authentication Dial-In User Service (RADIUS), RFC 2868 RADIUS Attributes for Tunnel Protocol Support и RFC 2869 RADIUS Extensions.

Список атрибутов IETF RADIUS, поддерживаемых коммутатором D-Link, приведен в таблице ниже.

Атрибуты аутентификации RADIUS:

Номер	Атрибут IETF
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
12	Framed-MTU
18	Reply-Message
24	State
26	Vendor-Specific
27	Session-Timeout
29	Termination-Action
30	Called-Station-ID
31	Calling-Station-ID
32	NAS-Identifier
60	CHAP-Challenge
61	NAS-Port-Type

64	Tunnel-Type
65	Tunnel-Medium-Type
77	Connect-Info
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID
85	Acct-Interim-Interval
87	NAS-Port-ID
95	NAS-IPv6-Address