Руководство пользователя (CLI)

Настраиваемые гигабитные коммутаторы уровня 2+

Коммутаторы серии ТГК-151

Версия 1.0

Москва
2022

Содержание

1. Введение

Описания команд в данном руководстве основаны на версии программного обеспечения 1.0. Перечисленные здесь команды представляют собой подмножество команд, поддерживаемых коммутатором серии ТГК-151.
В описании используется интерфейс технологического партнера, и некоторые надписи могут содержать названия и индексы, отличные от названий и индексов T-KOM. По мере выхода локализованного программного обеспечения, руководство будет корректироваться.

Аудитория

Это справочное руководство по интерфейсу командной строки предназначено для сетевых администраторов и других специалистов по ИТ-сетям, ответственных за управление коммутатором с помощью интерфейса командной строки (CLI). Интерфейс командной строки является основным интерфейсом управления коммутатором серии ТГК-151, который в данном руководстве обычно именуется просто «Коммутатор». Это руководство написано таким образом, что предполагается, что вы уже имеете опыт и знания в области Ethernet и современных сетевых принципов для локальных сетей.

Условные обозначения

Условное обозначение	**Описание**
Полужирный шрифт	Команды, опции команд и ключевые слова. Ключевые слова в командной строке необходимо вводить именно так, как они отображены.
КУРСИВ ЗАГЛАВНЫМИ	Параметры или значения, которые необходимо указать. Параметры в командной строке необходимо заменить желаемыми.
Квадратные скобки [ ]	Дополнительное значение или набор дополнительных аргументов
Фигурные скобки { }	Альтернативные ключевые слова, разделенные вертикальными линиями. Как правило, одно из ключевых слов в раздельных списках может быть выбрано.
Вертикальная линия |	Дополнительные значения или аргументы заключаются в квадратные скобки и разделяются вертикальной линией. Как правило, одно или более значение или аргумент в раздельных списках может быть выбрано.
Голубой шрифт Courier	Это соглашение используется для представления примера отображения консоли на экране, включая примеры ввода команд CLI с соответствующим выводом.

Предупреждения

Ниже представлены примеры трех типов предупреждений, которые могут использоваться в руководстве. При управлении коммутатором с помощью данного документа необходимо обращать внимание на эти предупреждения.

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 подключения к CLI коммутатора. Подключите разъем DB9 консольного кабеля (входит в комплект поставки) к последовательному (COM) порту компьютера. Подключите разъем RJ45 консольного кабеля к консольному порту коммутатора.

Для доступа к интерфейсу командной строки через консольный порт необходимо использовать программное обеспечение эмуляции терминала, такое как *PuTTY* или *Tera Term*. Коммутатор использует соединение со скоростью **115200** бит в секунду без включенного управления потоком.

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 опций или требуемых параметров и их использованием в команде.
- **По умолчанию** – если команда задает новое значение конфигурации или состояние коммутатора (например, отличное от используемого), это будет показано в данном поле.
- **Режим ввода команды** – режим, в котором возможно использование команды. Режимы описаны в разделе «Режимы ввода команд».
- **Уровень команды по умолчанию** – уровень привилегии пользователя, необходимый для использования команды.
- **Использование команды** – детальное описание команды и различных сценариев ее использования.
- **Пример** – 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 и уровня привилегий пользователя. Ввод вопросительного знака (?) после приглашения системы позволяет вывести список команд, доступных пользователю в определенном командном режиме.
Интерфейс командной строки поддерживает три уровня привилегий учетной записи пользователя:

- **Basic User** – 1 уровень привилегии. Данный уровень учетной записи пользователя имеет низший приоритет среди учетных записей. На данном уровне возможно получить доступ к просмотру базовой информации о системе.

- **Operator** – 12 уровень привилегии. На данном уровне учетной записи пользователя можно изменять локальные и глобальные настройки, не относящиеся к безопасности (например, настройки учетных записей пользователей, учетных записей SNMP и т.д.
- **Administrator** – 15 уровень привилегии. Учетная запись пользователя уровня Administrator имеет доступ ко всей информации о системе и системным настройкам, доступным в данном руководстве.

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

- User EXEC Mode (Пользовательский режим)
- Privileged EXEC Mode (Привилегированный режим)
- Global Configuration Mode (Режим глобальной конфигурации)

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

Режим ввода команд назначается сразу при входе пользователя в систему и зависит от уровня привилегий учетной записи. Сеанс начинается либо в режиме User EXEC Mode, либо в режиме **Privileged EXEC Mode**.

- Пользователи с **базовым** уровнем доступа **basic user** будут осуществлять вход в режиме **User EXEC Mode.**
- Пользователи с **расширенным** уровнем доступа: **Operator** и **Administrator** будут осуществлять вход в режиме **Privileged EXEC Mode.**

Соответственно, режим User EXEC Mode используется для Basic User, а режим Privileged EXEC Mode предоставляет функции уровня Operator и Administrator. Переход в режим Global Configuration Mode доступен только пользователям уровня Operator или Administrator.

Некоторые специальные режимы конфигурирования доступны только пользователям с максимальным уровнем прав, обладающим привилегиями самого высокого уровня безопасности на уровне Administrator.

В таблице кратко представлены доступные командные режимы, включая базовые и несколько специальных. Более подробно данные режимы рассматриваются в следующих главах руководства. Описания остальных специальных режимов в этом разделе не представлены. Для получения информации о дополнительных режимах настройки необходимо обратиться к главам, относящимся к этим функциям.
Доступные командные режимы и уровни привилегий:

Режим ввода команд / Уровень доступа	**Описание**
User EXEC Mode / Уровень Basic User	Самый низкий уровень приоритета среди пользовательских учетных записей. Доступ только к просмотру базовых настроек системы.
Privileged EXEC Mode / Уровень Operator	Изменение локальных и глобальных настроек терминала, контроль и выполнение некоторых задач администрирования. Исключен доступ к информации, относящейся к безопасности.
Privileged EXEC Mode / Уровень Administrator	Те же права, что и для уровня Operator, при этом пользователь также может просматривать и вносить изменения в настройки безопасности.
Global Configuration Mode / Уровень Operator	Применение глобальных настроек, за исключением настроек безопасности, для всей системы. Также используется для перехода к специальным режимам.

Global Configuration Mode / Уровень Administrator	Применение глобальных настроек для всей системы. Также используется для перехода к специальным режимам.
Interface Configuration Mode / Уровень Administrator	Режим настройки интерфейса.
VLAN Interface Configuration Mode	Режим настройки интерфейсов в VLAN.

User EXEC Mode с базовым уровнем доступа Basic User

Этот режим предназначен для проверки основных настроек системы. В данный режим можно войти с учетной записью Basic User.

Privileged EXEC Mode с уровнем доступа Operator

Данный режим позволяет получить доступ к глобальным настройкам и настройкам локального терминала, контролировать и решать задачи администрирования, за исключением настроек безопасности. Вход в данный режим можно получить, имея 12-й уровень привилегий.

Privileged EXEC Mode с уровнем доступа Administrator

Вход в данный режим можно получить, имея 15-й уровень привилегий. Поддерживается контроль и управление всей информацией о системе и настройках. Пользователь также может просматривать и вносить любые изменения в настройки безопасности.

Global Configuration Mode

Данный режим позволяет вносить изменения в глобальные настройки всей системы. Для входа в режим требуется учетная запись уровня Operator или Administrator. Настройки безопасности доступны только пользователям с учетной записью уровня Administrator. 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 войти в систему с соответствующим уровнем учетной записи и ввести команду **configure terminal** в привилегированном режиме Privileged EXEC.

В следующем примере выполняется вход в систему с учетной записью уровня Administrator в режиме Privileged EXEC и используется команда **configure terminal** для перехода в режим глобальной конфигурации:

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

Команда **exit** используется для выхода из режима глобальной конфигурации и возвращения к режиму Privileged EXEC.

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

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

Interface Configuration Mode (Режим конфигурирования интерфейса)

Режим конфигурирования интерфейса используется для настройки параметров одного или нескольких интерфейсов. В качестве интерфейса может выступать физический порт, VLAN или другой виртуальный интерфейс. Режим конфигурирования интерфейса различается в зависимости от типа интерфейса. Команды для каждого из типов интерфейсов немного отличаются.

VLAN Interface Configuration Mode (Режим конфигурирования интерфейса VLAN)

Режим конфигурирования интерфейсов VLAN используется для настройки параметров интерфейсов, назначенных VLAN.
Для доступа к режиму конфигурирования интерфейсов в VLAN необходимо использовать следующую команду в режиме глобальной конфигурации:

```
Switch(config)#interface vlan 1
Switch(config-if)#
```

Создание пользовательской учетной записи

Можно создать разные учетные записи пользователей для разных уровней. Этот раздел поможет пользователю создать учетную запись с помощью интерфейса командной строки.

Примечание: по умолчанию на коммутаторе уже настроена одна учетная запись пользователя. Имя пользователя и пароль для этой учетной записи – admin, уровень привилегий – 15.

После обновления микропрограммы коммутатора и создания учетных записей пользователей учетная запись **admin** по умолчанию будет автоматически создана после перезагрузки коммутатора с использованием нового файла конфигурации загрузки.

После обновления прошивки коммутатора и создания учетных записей пользователей учетная запись **admin** по умолчанию не будет создаваться автоматически. Только после сброса к заводским настройкам коммутатора будет создана учетная запись **admin** по умолчанию.

Рассмотрим следующий пример.

```
Switch>enable
Switch#configure terminal
Switch(config)#username user1 privilege 15 password 0 pass1234
Switch(config)#line console
Switch(config-line)#
```

В данном примере мы получили доступ к команде username.

В режиме User EXEC вводится команда **enable** для доступа к режиму Privileged EXEC.

- Далее используется команда **configure terminal** для перехода к глобальному режиму конфигурации. Данный режим позволяет использовать команду **username**.
- С помощью команды **username user1 privilege 15 password 0 pass1234** создается учетная запись пользователя с именем user1 и паролем pass1234, и назначается 15-й уровень привилегий для учетной записи user.
- Команда **line console** обеспечивает доступ к режиму конфигурации строки интерфейса.
- Команда **login local** сообщает коммутатору, что пользователям необходимо ввести локально настроенные учетные данные для входа в систему для доступа к интерфейсу консоли.

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

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

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

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

Switch#
```

Чтобы получить доступ к интерфейсу командной строки после перезагрузки коммутатора или выхода из учетной записи, необходимо ввести новое имя пользователя и пароль, как показано в примере ниже.

```
                DXS-1210-12SC 10GbE Smart Managed Switch

                          Command Line Interface
                         Firmware: Build V1.15.005
          Copyright(C) 2017 D-Link Corporation. All rights reserved.

User Access Verification

Username: admin
Password: *****
Switch#
```

Конфигурирование интерфейса

При конфигурировании физических портов коммутатора используется особое обозначение.

В следующем примере мы входим в режим глобальной конфигурации, далее переходим в режим конфигурации интерфейса Interface Configuration Mode, используя обозначение **1/0/1**. После входа в режим Interface Configuration Mode для порта 1 мы изменим скорость на 1 Гбит/с, используя команду **speed 1000**.

```
Switch# configure terminal
Switch(config)# interface Ethernet 1/0/1
Switch(config-if)# speed 1000
Switch(config-if)#
```

В примере используется обозначение 1/0/1. Терминология каждого параметра для интерфейса:

- UnitID/SlotID/IDпорта

Unit ID интерфейса указывает на номер коммутатора в стеке. Если стекирование отключено или настраиваемый коммутатор на включен в стек, то данный параметр не имеет значения. Slot ID интерфейса – это идентификатор модуля, подключенного к слоту расширения. ID порта интерфейса – это номер конфигурируемого физического порта.

Приведенный выше пример настройки позволяет сконфигурировать стекируемый коммутатор с ID 1, слотом 0 (Slot ID) и номером физического порта 1.

Сообщения об ошибке

Если коммутатор не распознает введенную команду, появятся сообщения об ошибке с основной информацией о проблеме. Список возможных ошибок представлен в таблице ниже.

Сообщение об ошибке	**Описание**
Ambiguous command	Введено недостаточно ключевых слов для распознавания команды.
Incomplete command	Введены не все требуемые ключевые слова 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 под курсором 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. Привыключении текст можно вставить в строку, а старый текст автоматически будет заменен новым.
Return	Прокручивает вниз на следующую строку или используется для ввода команды.
Пробел	Прокручивает вниз на следующую страницу или используется для ввода команды.

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

```
Switch# show running-config begin # AAA
#------------------------------------------------------------------------
#            DXS-1210-12SC 10GbE Smart Managed Switch Configuration
#
#                           Firmware: Build V1.15.005
#         Copyright(C) 2017 D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------
# AAA
end
configure terminal
no aaa new-model
end
# Dot1x
end
configure terminal
no dot1x system-auth-control
no snmp-server enable traps dot1x
interface ethernet 1/0/1
no dot1x pae authenticator
dot1x control-direction both
dot1x forward-pdu
dot1x max-req 2
dot1x timeout server-timeout 30
dot1x timeout supp-timeout 30
CTRL+C ESC q Quit SPACE n Next PageENTER Next Entry a All
```

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

```
Switch# show running-config include # AAA
#------------------------------------------------------------------------
#            DXS-1210-12SC 10GbE Smart Managed Switch Configuration
#
#                           Firmware: Build V1.15.005
#         Copyright(C) 2017 D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------
# AAA
Switch#
```

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

```
Switch# show running-config exclude # AAA
#------------------------------------------------------------------------
#            DXS-1210-12SC 10GbE Smart Managed Switch Configuration
#
#                           Firmware: Build V1.15.005
#         Copyright(C) 2017 D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------
# Basic
# LACP
configure terminal
lacp system-priority 32768
port-channel load-balance src-dst-mac
interface ethernet 1/0/1
lacp port-priority 32768
lacp timeout short
exit
interface ethernet 1/0/2
lacp port-priority 32768
lacp timeout short
exit
interface ethernet 1/0/3
lacp port-priority 32768
lacp timeout short
exit
CTRL+C ESC q Quit SPACE n Next PageENTER Next Entry a All
```

2. Основные команды CLI

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

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Команда help используется для получения краткой справочной информации, включая следующую:

- 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), потому что 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), потому что 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#
```

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

```
Switch#re?
reboot              reset

Switch#re
```

В следующем примере показано, как использовать справку **по синтаксису** команды для отображения следующего аргумента частично завершенной команды **telnet**. Символы, введенные до вопросительного знака (?), повторно печатаются в следующей командной строке, чтобы пользователь мог продолжить ввод команды.

```
Switch#telnet ?
A.B.C.D             IP address of a remote system
WORD                Telnet destination hostname
X:X:X:X::X          IPv6 address of a remote system

Switch#telnet
```

2-2 enable

Данная команда используется для входа в привилегированный режим EXEC (Privileged EXEC Mode).

enable [*PRIVILEGE-LEVEL***]**

Параметры

PRIVILEGE-LEVEL	(Опционально) Указывается уровень привилегий пользователя – от 1 до 15. Если значение не задано, используется уровень 15.

По умолчанию

Нет

Режим ввода команды

User EXEC Mode
Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется, если текущий уровень привилегий ниже уровня, необходимого для выполнения команды. Если привилегированный уровень требует пароля, введите его в предусмотренном для этого поле. Разрешено только 3 попытки. При неудачном вводе пользователь будет возвращен к текущему уровню.

Пример

В этом примере показано, как войти в режим Privileged EXEC.

```
Switch# enable 15
password:***
Switch#
```

2-3 disable

Данная команда используется для изменения уровня привилегии активной сессии учетной записи CLI на более низкий.

disable [*PRIVILEGE-LEVEL***]**

Параметры

PRIVILEGE-LEVEL	(Опционально) Указывается уровень привилегий. Если значение не задано, используется уровень 1.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду, чтобы ввести уровень привилегий, который ниже текущего уровня. При использовании этой команды для входа на уровень привилегий, для которого настроен пароль, пароль не требуется.

Пример

В этом примере показано, как выйти из системы.

```
Switch# disable
Switch> logout
```

2-4 configure terminal

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

configure terminal

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для входа в режим глобальной конфигурации.

Пример

В данном примере показан процесс входа в режим глобальной конфигурации.

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

2-5 login (EXEC)

Данная команда используется для настройки имени пользователя.

Login

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется 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 показан процесс входа в учетную запись с именем пользователя «user1».

```
Switch# login

Username: user1
Password: xxxxx

Switch#
```

2-6 login (Line)

Данная команда используется для настройки метода входа для указанного типа подключения. Используйте форму **no** для отключения требования авторизации.

login [local]
no login

Параметры

local	(Опционально) Укажите, чтобы использовать локальную базу данных при аутентификации.

По умолчанию

По умолчанию все линейные интерфейсы используют локальный метод входа (по имени пользователя и паролю).

Режим ввода команды

Line Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Для доступа через консоль и по Telnet при включении аутентификации AAA используются правила, сконфигурированные модулем AAA. Если аутентификация AAA отключена, применяются следующие правила:

- При выключении авторизации пользователь войдет в систему с уровнем привилегий 1.
- При выборе опции **by password** после ввода того же пароля, что в команде **password,** пользователь войдет в строку на уровне 1. Если пароль не был сконфигурирован, будетотображено сообщение об ошибке и сессия будет завершена.
- При выборе опции **username and password**, введите имя пользователя и пароль,сконфигурированные командой **username.**

Для доступа по SSH используется 3 типа аутентификации:

- аутентификация с использованием открытого ключа SSH,
- аутентификация на основе узла,
- аутентификация с помощью пароля.

К типам аутентификации с помощью открытого ключа и на основе узла указанные ниже правила не применяются, в отличие от аутентификации с помощью пароля, для которой необходимо учитывать следующие правила:

- При включении AAA используется модуль AAA.
- При выключении AAA используются следующие правила:

- Если возможность входа отключена, имя пользователя и пароль игнорируются. Ввод деталей на уровне 1.
- Если выбрана опция **username and password**, введите имя пользователя и пароль,сконфигурированные командой **username.**
- При выборе опции **password** имя пользователя игнорируется, но требуется ввод пароля,использованного в команде **password,** для входа в систему на уровне 1.

Пример

В данном примере показано, как перейти в режим конфигурации строки (Line Configuration Mode) и создать пароль пользователя для входа на коммутатор. Этот пароль начнет действовать только после того, как соответствующая строка будет настроена на авторизацию.

```
Switch# configure terminal
Switch(config)# line console
Switch(config-line)# password loginpassword
Switch(config-line)#
```

В данном примере показано, как настроить авторизацию в качестве метода входа на коммутатор.

```
Switch# configure terminal
Switch(config)# line console
Switch(config-line)# login
Switch(config-line)#
```

В данном примере показан процесс ввода команды login. Устройство проверит подлинность пользователя на основе ввода пароля. При корректном вводе пользователь получит доступ определенного уровня.

```
Switch#login

Password:*************

Switch#
```

В данном примере показан процесс создания имени пользователя «useraccount» с паролем «pass123»и уровнем привилегий 12.

```
Switch# configure terminal
Switch(config)# username useraccount privilege 12 password 0 pass123
Switch(config)#
```

В данном примере показан процесс конфигурации метода входа login local.

```
Switch# configure terminal
Switch(config)# line console
Switch(config-line)# login local
Switch(config-line)#
```

2-7 logout

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

logout

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

В данном примере показан процесс выхода из системы.

```
Switch# disable
Switch# logout
```

2-8 end

Данная команда используется для выхода из текущего режима конфигурации и возвращения к высшему режиму в иерархии CLI, т. е. к пользовательскому (User EXEC Mode) или привилегированному режиму (Privileged EXEC Mode).

end

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode.
Любой режим конфигурации.

Уровень команды по умолчанию

Уровень 1

Использование команды

Выполнение этой команды вернет доступ к самому верхнему режиму в иерархии CLI, независимо от того, в каком режиме конфигурации или подрежиме конфигурации находится в данный момент.

Пример

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

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

2-9 exit

Данная команда используется 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.

exit

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду для выхода из текущего режима конфигурации и возврата в предыдущий режим. Если пользователь находится в режиме User EXEC Mode или Privileged EXEC Mode, эта команда приведет к выходу из сеанса.

Пример

В данном примере показан процесс возвращения из режима конфигурации интерфейса Interface Configuration Mode в режим глобальной конфигурации Global Configuration Mode.

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

2-10 show history

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

show history

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Все введенные команды сохраняются в системе. Для повторного вызова сохраненной команды используется сочетание клавиш CTRL+P или клавиша Вверх. В этом случае команды вызываются последовательно, начиная с последних команд. 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#
```

2-11 show environment

Данная команда используется для отображения информации об охлаждении, температуре и питании.

show environment [fan | power | temperature]

Параметры

fan	(Опционально) Отображение детальной информации о состоянии вентиляторов.
power	(Опционально) Отображение детальной информации о питании.
temperature	(Опционально) Отображение детальной информации о температуре.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Если не указан определенный тип, отображаться будут все типы информации.

Пример

В данном примере показано отображение информации о состоянии вентиляторов, температуре и питании устройства.

```
Switch#show environment

Detail Temperature Status:
Unit     Temperature Descr/ID          Current/Threshold Range
-----    ----------------------------------------------------
1         Central Temperature/1         24C/0~45C
Status code: * temperature is out of threshold range

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

Detail Power Status:
Unit     Power Module       Power Status
-----    ----------------   -------------
1        Power 1            in-operation
1        Power 2            empty

Switch#
```

Отображаемые параметры

Power Status	**in-operation:** источник питания работает нормально. **empty**: источник питания не подключен. **failed**: Силовой стабилизатор не работает нормально.

2-12 show unit

Данная команда позволяет получить общую информацию о системе.

show unit [*UNIT-ID***]**

Параметры

UNIT-ID	(Опционально) Укажите номер устройства в стеке, для которого необходимо получить информацию.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для просмотра информации об устройствах стека. Если параметр UNIT- ID не указан, выводится информация обо всех устройствах.

Пример

В этом примере показано, как отобразить информацию об устройствах в системе.

```
Switch#show unit

Unit         Model Descr                              Model Name
----  ---------------------------------------  ------------------------------
 1     24P 10/100/1000 with 4P Combo 4P SFP+        DGS-3130-30TS

Unit         Serial-Number                 Status        Up Time
----  --------------------------------  ---------  -----------------
 1     DGS3130102030                     ok          0DT0H23M9S

Unit   Memory     Total       Used        Free
----  --------  ----------  ----------  ----------
 1     DRAM     1048576 K    377313 K    671263 K
 1     FLASH    1039872 K     45812 K    994060 K

Switch#
```

2-13 show cpu utilization

Данная команда позволяет получить информацию об использовании CPU.

show cpu utilization

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда отображает данные по загрузке центрального процессора за последние 5 секунд, 1 минуту и 5 минут.

Пример

В данном примере показано получение информации о загрузке процессора.

```
Switch#show cpu utilization

CPU Utilization

Five seconds -  12 %        One minute -  12 %        Five minutes -  12 %

Switch#
```

2-14 show version

Данная команда позволяет получить информацию о версии программного обеспечения и аппаратной ревизии устройства.

show version

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда выводит информацию о версии системного ПО, загрузочного ПО и аппаратной ревизии устройства.

Пример

В данном примере показано отображение информации о коммутаторе.

```
Switch#show version

System MAC Address: 3C-1E-04-A1-B9-E0

Unit ID    Module Name           Versions
-------  ----------------  --------------------
   1      DGS-1510-28XMP      H/W:A1
                              Bootloader:1.00.016
                              Runtime:1.70.005


Switch#
```

2-15 snmp-server enable traps environment

Данная команда позволяет получать трапы о состоянии питания, температуре и работе вентиляторов. Для отключения данной команды используйте форму **no**.

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

Параметры

fan	(Опционально) Укажите для получения трапов о состоянии вентиляторов, чтобы получать предупреждения о событиях (остановка вентилятора или восстановление работы вентилятора).
power	(Опционально) Укажите для получения трапов о состоянии питания, чтобы получать предупреждения о событиях (отказ питания или восстановление питания). Эти трапы можно отправлять только через порты 10G.
temperature	(Опционально) Укажите для получения трапов о состоянии температуры, чтобы получать предупреждение о событиях (превышение допустимых параметров температуры или восстановление температуры).

По умолчанию

По умолчанию поддержка трапов для данных параметров отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет получать трапы о состоянии питания, температуре и работе вентиляторов. Если не указан определенный параметр, включается поддержка трапов для всех параметров.

Пример

В данном примере показан процесс включения трапов.

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

2-16 environment temperature threshold

Данная команда позволяет настроить пороговые значения температур для срабатывания термодатчика. При использовании формы **no** система вернется к настройкам по умолчанию.

environment temperature threshold unit *UNIT-ID* **thermal** *THERMAL-ID* **[high** *VALUE***] [low** *VALUE***]**
no environment temperature threshold unit *UNIT-ID* **thermal** *THERMAL-ID* **[high] [low]**

Параметры

unit *UNIT-ID*	Укажите UNIT-ID.
thermal *THERMAL-ID*	Укажите идентификатор термодатчика.
high	(Опционально) Укажите верхнюю границу температуры в градусах Цельсия. Доступен диапазон от -100 до 200.
low	(Опционально) Укажите нижнюю границу температуры в градусах Цельсия. Доступен диапазон от -100 до 200. Нижняя граница не может быть выше верхней границы.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет настроить пороговые значения температуры окружающей среды внутри устройства, соответствующие нормальному 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 показан процесс настройки диапазона температуры для термосенсора ID 1 в устройстве Unit 1.

```
Switch# configure terminal
Switch(config)# environment temperature threshold unit 1 thermal 1 high 100 low 20
Switch(config)#
```

2-17 privilege

Эта команда используется для настройки прав выполнения командной строки на уровень привилегий. Используйте форму **no** этой команды, чтобы вернуть командную строку к уровню настройки по умолчанию.

privilege *MODE* **{level** *PRIVILEGE-LEVEL* **| reset }** *COMMAND-STRING*
no privilege *MODE COMMAND-STRING*

Параметры

MODE	Указывает режим работы команды.
level *PRIVILEGE-LEVEL*	Указывает уровень права на выполнение. Значение составляет от 1 до 15.
reset	Указывает на возврат команды к уровню настройки по умолчанию.
COMMAND-STRING	Указывает команду, которую необходимо изменить.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Эта команда используется для настройки прав выполнения командной строки на уровень привилегий. Когда используется эта команда, используемая командная строка должна существовать на текущем уровне команд. Если более одной команды начинаются с указанной командной строки, все команды, начинающиеся с этой командной строки, будут изменены на указанный командный уровень.

Пример

В этом примере показано, как настроить командную строку configure terminal как команду уровня 1.

```
Switch#configure terminal
Switch(config)#privilege exec level 1 configure terminal
Switch(config)#
```

2-18 show privilege

Данная команда используется для отображения текущего уровня привилегий.

show privilege

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения текущего уровня привилегий.

Пример

В данном примере показано, как отобразить информацию о текущем уровне привилегий.

```
Switch#show privilege

Current privilege level is 15

Switch#
```

3. Команды 802.1X

3-1 clear dot1x counters

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

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

Параметры

all	Обнуление счетчиков 802.1X (диагностика, статистика и статистика сессии) на всех интерфейсах.
interface INTERFACE-ID	Обнуление 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 отдельных интерфейсов и их групп. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

В данном примере показан процесс обнуления всех счетчиков 802.1X (диагностика, статистика и статистика сессии) на Ethernet 1/0/1.

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

3-2 dot1x control-direction

Данная команда используется для настройки типа трафика на порту как однонаправленного (in) или двунаправленного (both). При использовании формы **no** команда вернет настройки по умолчанию.

dot1x control-direction {both | in}
no dot1x control-direction

Параметры

both	Включение контроля трафика в двух направлениях.
in	Включение контроля трафика в одном направлении.

По умолчанию

По умолчанию используется двунаправленный режим.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может использоваться только для настройки интерфейса 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, 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.

Пример

В данном примере показан процесс настройки контроля трафика на интерфейсе Ethernet 1/0/1 как однонаправленного.

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

3-3 dot1x default

Данная команда используется 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.
Максимум запросов – 2 раза.
Таймер сервера – 30 секунд.
Таймер запроса – 30 секунд.
Интервал передачи – 30 секунд.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для возврата параметров IEEE 802.1X определенного порта к настройкам по умолчанию. Команда доступна только для интерфейсов физического порта.

Пример

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

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# dotlx default
Switch(config-if)#
```

3-4 dot1x port-control

Данная команда используется для управления состоянием авторизации порта. При использовании формы **no** данная команда вернет все к значениям по умолчанию.

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

Параметры

auto	Включение аутентификации IEEE 802.1X для порта.
force-authorized	Порт считается принудительно авторизованным.
force-unauthorized	Порт считается принудительно неавторизованным.

По умолчанию

По умолчанию данная опция настроена как **auto**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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.

Данная команда доступна только для конфигурации интерфейса 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**, управление портом в указанном направлении заблокировано.

Пример

В данном примере показан процесс запрета любого доступа на Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
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. При использовании формы **no** данная команда отключит функцию продвижения кадров dot1x PDU.

dot1x forward-pdu
no dot1x forward-pdu

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурации интерфейса физического порта. Команда работает, 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 ethernet 1/0/1
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	Порт, на котором будет инициирована аутентификация. Доступными интерфейсами являются физические порты.
,	(Опционально) Используется для перечисления отдельных интерфейсов и их групп. Пробелы до и после запятой недопустимы.
-	(Опционально) Указывается для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы
mac-address *MAC-ADDRESS*	Указание MAC-адреса для инициализации.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

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 показан процесс инициализации режима аутентификатора для Ethernet 1/0/1.

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

3-7 dot1x max-req

Данная команда позволяет задать максимальное количество попыток для передачи клиенту запроса EAP (Extensive Authentication Protocol) от внутреннего сервера аутентификации, прежде чем инициировать повторную аутентификацию. При использовании формы **no** данная команда вернет настройки по умолчанию.

dot1x max-req *TIMES*
no dot1x max-req

Параметры

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

По умолчанию

По умолчанию используется значение 2

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурации интерфейса физического порта. Если клиент не отвечает на запрос аутентификации в течение периода, заданного командой **dot1x timeout tx-period** *SECONDS*, коммутатор отправит повторный запрос. Данная команда позволяет 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 равное 3.

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

3-8 dot1x pae authenticator

Данная команда используется для конфигурации определенного порта в качестве аутентификатора IEEE 802.1X PAE (Port Access Entity). При использовании формы **no** данная команда отключит использование порта в качестве аутентификатора IEEE 802.1X.

dot1x pae authenticator
no dot1x pae authenticator

Параметры

Нет

По умолчанию

По умолчанию эта опция отключена

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурации интерфейса 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 показан процесс конфигурации Ethernet 1/0/1 в качестве аутентификатора IEEE 802.1X PAE.

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

В данном примере показан процесс отключения аутентификации IEEE 802.1X для интерфейса Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
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*	Указывает порт для повторной аутентификации. Доступными интерфейсами являются физические порты.

,	(Опционально) Используется для перечисления отдельных интерфейсов или групп интерфейсов. Пробелы до и после запятой недопустимы.
-	(Опционально) Указывается для обозначения диапазона интерфейсов. Пробелы до и после дефиса.
mac-address *MAC-ADDRESS*	Указание MAC-адреса для повторной аутентификации.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

В данном примере показан процесс включения повторной аутентификации для интерфейса Ethernet 1/0/1.

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

3-10 dot1x system-auth-control

Данная команда используется для глобального включения аутентификации IEEE 802.1X на коммутаторе. При использовании формы **no** данная команда отключит аутентификацию IEEE 802.1X.

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

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Функция аутентификации IEEE 802.1X не позволяет неавторизованным узлам 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 показан процесс включения глобальной аутентификации IEEE 802.1X.

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

3-11 dot1x timeout

Данная команда используется для настройки таймеров IEEE 802.1X. При использовании формы **no** данная команда вернет все значения по умолчанию.

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

Параметры

server-timeout *SECONDS*	Период времени в секундах, в течение которого коммутатор ожидает запрос от сервера аутентификации. По истечении времени ожидания аутентификатор отправит клиенту пакет EAP-Request. Доступен диапазон значений от 1 до 65535.
supp-timeout *SECONDS*	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. Доступен диапазон значений от 1 до 65535.
tx-period *SECONDS*	Период времени в секундах, в течение которого коммутатор ожидает ответ на запрос EAP-Request/Identity от клиента перед повторной отправкой запроса. Доступен 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурации интерфейса 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 ethernet 1/0/1
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) Интерфейс или группа интерфейсов, для которых будет отображаться конфигурация dot1x. Если значение не указано, отображаться будет глобальная конфигурация.
,	(Опционально) Используется для перечисления отдельных интерфейсов или групп интерфейсов. Пробелы до и после запятой недопустимы.
-	(Опционально) Указывается для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения глобальной конфигурации или конфигурации интерфейса. Если введена команда без параметров, отображаться будет глобальная конфигурация. В противном случае отображаться будет конфигурация определенного интерфейса.

Пример

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

```
Switch#show dot1x

802.1X                  : Enabled
Trap State              : Enabled

Switch#
```

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

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


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) Интерфейс или группа интерфейсов, для которых будут отображаться параметры диагностики dot1x. Если значение не указано, отображается информация обо всех интерфейсах.
,	(Опционально) Используется для перечисления отдельных интерфейсов или групп интерфейсов. Пробелы до и после запятой недопустимы.
-	(Опционально) Указывается для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения результатов диагностики IEEE 802.1X. Если значение не указано, отображаться будут данные для всех интерфейсов. В противном случае отображаются данные диагностики для заданного интерфейса.

Пример

В примере показано, как вывести данные диагностики dot1X для Ethernet-порта 1/0/1.

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

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) Интерфейс или группа интерфейсов, для которых будет отображаться статистика dot1x. Если значение не указано, отображаться будет информация для всех интерфейсов.
,	(Опционально) Используется для перечисления отдельных интерфейсов или групп интерфейсов. Пробелы до и после запятой недопустимы.
-	(Опционально) Указывается для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения статистики IEEE 802.1X. Если значение не указано, отображаться будет статистика для всех интерфейсов.

Пример

В данном примере показано, как включить отображение статистики dot1X для Ethernet-порта 1/0/1.

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

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) Интерфейс или группа интерфейсов, для которых будет отображаться статистика сессии dot1x. Если значение не указано, отображаться будет информация для всех интерфейсов.
,	(Опционально) Используется для перечисления отдельных интерфейсов или групп интерфейсов. Пробелы до и после запятой недопустимы.
-	(Опционально) Указывается для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

В этом примере показано, как отобразить статистику сеанса dot1X на порту 1.

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

eth6/0/1 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 для включения отправки уведомлений SNMP для аутентификации 802.1X. При использовании формы no данная команда отключит отправку уведомлений SNMP.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда может использоваться для включения или отключения отправки SNMP-уведомлений для аутентификации 802.1X.

Пример

В данном примере показан процесс включения отправки трапов для аутентификации 802.1X.

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

4. Команды списка контроля доступа (ACL)

4-1 access-list resequence

Данная команда используется для того, чтобы повторно задать начальный порядковый номер и для увеличения числа записей в списке доступа. При использовании формы **no** команда вернется к значениям по умолчанию.

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

Параметры

NAME	Имя конфигурируемого списка доступа. Может содержать максимум 32 символа.
NUMBER	Указывает номер конфигурируемого списка доступа.
STARTING-SEQUENCE-NUMBER	Указывает, что записи списка доступа будут перегруппированы с использованием этого начального значения. Значение по умолчанию – 10 Доступен диапазон значений от 1 до 65535.
INCREMENT	Задает шаг порядковых номеров. Значение по умолчанию – 10 Например, если значение шага – 5, а начальный номер – 20, последующими числами будут 25, 30, 35, 40 и т. д. Доступен 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная функция позволяет пользователю повторно упорядочить записи указанного списка доступа с начальным порядковым номером записи, определяемым параметром *STARTING-SEQUENCE-NUMBER*, а значение шага задается с помощью параметра *INCREMENT*. Если наибольшее значение порядкового номера превышает максимально возможное значение, то существующие порядковые номера не изменятся.

Если правило создано без указания определенного порядкового номера, он будет присвоен автоматически. Если это первая запись, то будет присвоен начальный порядковый номер. Последующим записям правила назначается номер, больший на значение шага; а самый большой порядковый номер в списке доступа будет стоять в конце.

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 показан процесс изменения порядкового номера списка доступа IP-адресов (IP access-list) с именем R&D.

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

4-2 acl-hardware-counter

Эта команда используется для включения аппаратного счетчика ACL указанного имени списка доступа для функций группы доступа или карты доступа для функции фильтра VLAN. Используйте форму **no** этой команды для отключения функции аппаратного счетчика ACL.

acl-hardware-counter {access-group {*ACCESS-LIST-NAME* **|** *ACCESS-LIST-NUMBER***} | vlan- filter** *ACCESS-MAP-NAME***}**

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

Параметры

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

vlan- filter *ACCESS-MAP-NAME*	Указывает имя настраиваемой карты доступа.

По умолчанию

По умолчанию эта опция отключена

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда с параметром **access-group** включит аппаратный счетчик ACL для всех портов, к которым применено указанное имя или номер списка доступа. Подсчитывается количество пакетов, соответствующих каждому правилу.

Команда с параметром **vlan-filter** включит аппаратный счетчик ACL для всех VLAN, к которым применена указанная карта доступа VLAN. Подсчитывается количество пакетов, разрешенных каждой картой доступа.

Пример

В этом примере показано, как включить аппаратный счетчик ACL.

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

4-3 action

Данная команда используется для настройки действий продвижения, отбрасывания или переадресации из sub-map в режиме VLAN Access-map Sub-map Configuration Mode. При использовании формы **no** данная команда вернется к настройкам по умолчанию.

action {forward | **drop** | **redirect** *INTERFACE-ID***}**
no action

Параметры

forward	Укажите для продвижения пакета при совпадении.
drop	Укажите для отбрасывания пакета при совпадении.
redirect *INTERFACE-ID*	Укажите ID интерфейса для перенаправления. Указать можно только физические порты.

По умолчанию

Параметр по умолчанию – **forward**.

Режим ввода команды

VLAN Access-map Sub-map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Для одной sub-map доступно только одно действие. Действие, заданное позже, заменит предыдущее. VLAN access map может содержать несколько sub-map. Пакет, совпадающий с sub-map (пакет, разрешенный соответствующим списком доступа) примет действие, указанное для sub-map. Дальнейшая проверка следующих sub-map производиться не будет. Если пакет не совпадает с sub-map, проверяться будет следующая sub-map.

Пример

В данном примере показан процесс конфигурации действия на sub-map.

```
Switch# show vlan access-map
VLAN access-map vlan-map 20
  match mac address: ext_mac(ID: 6856)
  action: forward
Switch# configure terminal
Switch(config)# vlan access-map vlan-map 20
Switch(config-access-map)# action redirect ethernet 1/0/5
Switch(config-access-map)# end
Switch# show vlan access-map
VLAN access-map vlan-map 20
  match mac address:  ext_mac(ID: 6856)
  action: redirect eth1/0/5
Switch#
```

4-4 clear acl-hardware-counter

Эта команда используется для очистки аппаратного счетчика ACL.

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

Параметры

access-group *ACCESS-LIST-NAME*	Указывает имя списка доступа, который необходимо очистить.
access-group *ACCESS-LIST-NUMBER*	Указывает номер конфигурируемого списка доступа.
vlan- filter *ACCESS-MAP-NAME*	Указывает имя карты доступа, которую необходимо очистить.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если с параметром **access-group** не указано имя или номер списка доступа, все аппаратные счетчики группы доступа будут очищены. Если с параметром **vlan-filter** не указано имя карты доступа, все аппаратные счетчики фильтра VLAN будут очищены.

Пример

В этом примере показано, как очистить аппаратный счетчик ACL.

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

4-5 expert access-group

Эта команда используется для применения определенного экспертного ACL к интерфейсу. Используйте форму **no** этой команды для отмены применения.

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

Параметры

NAME	Имя настраиваемого списка управления доступом expert (expert access-list). Максимальное число допустимых символов в имени – 32
NUMBER	Указывает номер настраиваемого экспертного списка доступа.
in	(Опционально) Фильтрация входящих пакетов на интерфейс. Если направление не указано, используется значение **in**.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если экспертная группа доступа уже настроена на интерфейсе, команда, примененная позже, перезапишет предыдущую настройку. Только один список доступа одного типа может быть применен к одному интерфейсу; но списки доступа разных типов могут быть применены к одному интерфейсу.

Ресурсы диапазона VLAN и диапазона портов 4-го уровня являются общими. После успешного применения команды будет показано количество оставшихся записей в диапазоне.

Пример

В этом примере показано применение экспертного ACL "exp_acl" к порту 2.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#expert access-group exp_acl in

 PROMPT: The remaining applicable EXPERT related access entries are 256, remaining
range entries are 32.
Switch(config-if)#
```

4-6 expert access-list

Данная команда используется для создания или изменения расширенного списка управления доступом expert (extended expert ACL). Использование данной команды осуществляет вход в режим Extended Expert Access-List Configuration Mode. При использовании формы **no** команда удалит расширенный список доступа Expert.

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

Параметры

NAME	Имя конфигурируемого расширенного списка доступа expert. Максимальное число допустимых символов в имени – 32.
NUMBER	Идентификационный номер (ID number) экспертного списка доступа. Для расширенных списков доступа expert допустимо значение от 8000 до 9999.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Имя каждого списка доступа должно быть уникальным. Все символы, используемые в имени, чувствительны к регистру. Если номер списка доступа не указан, автоматически будет назначен самый большой неиспользуемый номер из диапазона номеров списка доступа expert (expert access list numbers).

Пример

В данном примере показано, как создать расширенный список управления доступом expert.

```
Switch# configure terminal
Switch(config)# expert access-list extended exp_acl
Switch(config-exp-nacl)# end
Switch# show access-list
Access-List-Name                     Type
------------------------------------ ---------------
exp_acl(ID: 8999)                    expert ext-acl

Total Entries: 1

Switch#
```

4-7 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]**
no ip access-group [*NAME* **|** *NUMBER***] [in]**

Параметры

NAME	Имя используемого списка доступа IP. Максимальное число допустимых символов в имени – 32
NUMBER	Указывает номер применяемого списка доступа IP.
in	(Опционально) Указывает, что список доступа IP будет применен для проверки пакетов во входящем направлении. Если направление не указано, используется **in**.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если группа доступа IP (IP access group) уже настроена на интерфейсе, примененная позднее команда заменит предыдущие настройки. К каждому интерфейсу можно применить только один список доступа определенного типа, но списки доступа различных типов могут быть применены к одному и тому же интерфейсу.

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

Пример

В данном примере показан процесс настройки списка доступа IP «Strict-Control» в качестве группы доступа IP для Ethernet 1/0/2.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/2
Switch(config-if)#ip access-group Strict-Control

The remaining applicable IP related access entries are 1792, remaining range entries are 32.
Switch(config-if)#
```

4-8 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. При использовании формы **no** команда удалит список доступа IP.

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

Параметры

extended	(Опционально) Указывает, что список доступа IP является расширенным списком доступа IP (extended IP access list) и есть возможность применить больше опций фильтрации. Если параметр не указан, список доступа будет считаться стандартным.
NAME	Назначаемое имя списка доступа IP. Максимальное число допустимых символов в имени – 32.
NUMBER	Указывает идентификационный номер списка доступа IP. Для стандартных списков доступа IP это значение составляет от 1 до 1999. Для расширенных списков доступа IP это значение составляет от 2000 до 3999.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

4-9 ipv6 access-group

Данная команда используется для применения списка доступа IPv6 (IPv6 access list) на интерфейсе.При использовании формы **no** команда удалит список доступа IPv6.

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

Параметры

NAME	Указывает имя применяемого списка доступа IPv6.
NUMBER	Указывает номер применяемого списка доступа IPv6.
in	Указывает, что список доступа IPv6 будет применяться к проверке в направлении входа. Если направление не указано, используется используется.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

К каждому интерфейсу можно применить только один список доступа определенного типа, но списки доступа различных типов могут быть применены к одному интерфейсу. Привязка группы доступа (access

group) к интерфейсу будет расходовать ресурсы из записей фильтрации коммутатора. Если ресурсов недостаточно для активации команды, появится сообщение об ошибке.

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

Пример

В этом примере показано, как указать список доступа IPv6 "ip6-control" в качестве группы доступа IP для порта 3.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/3
Switch(config-if)#ipv6 access-group ip6-control in

The remaining applicable IPv6 related access entries are 448, remaining range entries are 32.
Switch(config-if)#
```

4-10 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. При использовании формы **no** команда удалит список доступа IPv6.

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

Параметры

extended	(Опционально) Указывает, что список доступа IPv6 является расширенным списком доступа IPv6 и есть возможность применить больше опций фильтрации. Если параметр не указан, список доступа IPv6 будет считаться стандартным.
NAME	Назначаемое имя списка доступа IPv6. Максимальное число допустимых символов в имени – 32.
NUMBER	Указывает идентификационный номер списка доступа IPv6. Для стандартных списков доступа IPv6 это значение составляет от 11000 до 12999. Для расширенных списков доступа IPv6 это значение составляет от 13000 до 14999.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 extended access list) с 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 standard access list) с 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)#
```

4-11 list remark

Эта команда используется для добавления примечаний для указанного ACL. Используйте форму **no** этой команды, чтобы удаления примечаний.

list-remark *TEXT*
no list-remark

Параметры

TEXT	Указывает информацию о замечании. Длина информации может составлять до 256 символов.

По умолчанию

Нет

Режим ввода команды

Access-list Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда доступна в режимах MAC, IP, IPv6 и Expert Access-list Configure.

Пример

В этом примере показано, как добавить примечание 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#
```

4-12 mac access-group

Данная команда используется для применения списка управления доступом MAC (MAC access list) к интерфейсу. Для удаления группы доступа с интерфейса воспользуйтесь формой **no**.

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

Параметры

NAME	Укажите имя используемого списка доступа MAC.
NUMBER	Укажите номер используемого списка доступа MAC.
in	(Опционально) Указывает, что список доступа MAC будет применен для проверки пакетов во входящем направлении. Если направление не указано, используется значение **in**.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если группа доступа MAC (MAC access group) уже настроена на интерфейсе, следующая команда перезапишет предыдущие настройки. Группы доступа MAC не проверяют IP- пакеты.

К каждому интерфейсу можно применить только один список доступа определенного типа, но списки доступа различных типов могут быть применены к одному интерфейсу.

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

Пример

В данном примере показано применение списка доступа MAC daily-profile к порту 1/0/5.

```
Switch#configure terminal
Switch(config)#interface eth1/0/5
Switch(config-if)#mac access-group daily-profile in

 PROMPT: The remaining applicable MAC related access entries are 448, remaining
range entries are 32.
Switch(config-if)#
```

4-13 mac access-list

Данная команда используется для создания или изменения списков управления доступом MAC (MAC access list). Команда позволяет войти в режим MAC Access List Configuration Mode. Для удаления списка доступа MAC воспользуйтесь формой **no**.

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

Параметры

NAME	Укажите имя конфигурируемого списка доступа MAC. Максимальное число допустимых символов в имени – 32.
NUMBER	Укажите ID-номер (ID number) списка доступа MAC. Для расширенных списков доступа MAC диапазон значений от 6000 до 7999.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы войти в режим MAC Access-List Configuration Mode, и введите команду **permit** или **deny**, чтобы указать записи. Имя каждого списка доступа должно быть уникальным. 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 MAC.

Пример

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

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

4-14 match ip address

Эта команда используется для привязки списка доступа IP для настроенной подкарты. Форма **no** этой команды удаляет запись соответствия.

match ip address {*ACL-NAME* **|** *ACL-NUMBER***}**
no match ip address

Параметры

ACL-NAME	Указывает имя настраиваемого списка доступа ACL. Имя может содержать до 32 символов.
ACL-NUMBER	Указывает номер конфигурируемого списка доступа IP ACL.

По умолчанию

Нет

Режим ввода команды

VLAN Access-map Sub-map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду, чтобы связать список доступа IP с настроенной подкартой. Одна подкарта может быть связана только с одним списком доступа (список доступа IP, список доступа IPv6 или список доступа MAC). IP-подкарта только проверяет IP-пакеты. Более новая команда перезаписывает предыдущую настройку.

Пример

В этом примере показано, как настроить содержимое соответствия в подкарте.

```
Switch# configure terminal
Switch(config)# vlan access-map vlan-map 20
Switch(config-access-map)# match ip address sp1
Switch(config-access-map)#
```

4-15 match ipv6 address

Эта команда используется для привязки списков доступа IPv6 к настроенным подкартам. Форма **no** этой команды удаляет запись соответствия.

match ipv6 address {ACL-NAME | ACL-NUMBER}
no match ipv6 address

Параметры

ACL-NAME	Указывает имя настраиваемого списка доступа ACL. Имя может содержать до 32 символов.
ACL-NUMBER	Указывает номер конфигурируемого списка доступа IP ACL.

По умолчанию

Нет

Режим ввода команды

VLAN Access-map Sub-map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду, чтобы связать список доступа IPv6 с настроенной подкартой. Одна подкарта может быть связана только с одним списком доступа (список доступа IP, список доступа IPv6 или список доступа MAC). Подкарта IPv6 только проверяет пакеты IPv6. Последующая команда перезаписывает предыдущую настройку.

Пример

В этом примере показано, как установить содержимое соответствия в подкарте.

```
Switch# configure terminal
Switch(config)# vlan access-map vlan-map 20
Switch(config-access-map)# match ipv6 address sp1
Switch(config-access-map)#
```

4-16 match mac address

Эта команда используется для ассоциирования списков доступа MAC для настроенных подкарт. Форма **no** этой команды удаляет запись соответствия.

match mac address {*ACL-NAME* **|** *ACL-NUMBER***}**
no match mac address

Параметры

ACL-NAME	Указывает имя настраиваемого списка доступа ACL. Имя может

	содержать до 32 символов.
ACL-NUMBER	Указывает номер конфигурируемого списка доступа IP ACL.

По умолчанию

Нет

Режим ввода команды

VLAN Access-map Sub-map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду, чтобы связать список доступа MAC с настроенной подкартой. Одна подкарта может быть связана только с одним списком доступа (список доступа IP, список доступа IPv6 или список доступа MAC). MAC-подкарта только проверяет пакеты, не относящиеся к IP. Последующая команда перезаписывает предыдущую настройку.

Пример

В этом примере показано, как установить содержимое соответствия в sub-map.

```
Switch# configure terminal
Switch(config)# vlan access-map vlan-map 30
Switch(config-access-map)# match mac address ext_mac
Switch(config-access-map)#
```

4-17 permit | deny (expert access-list)

Данная команда используется для добавления записи разрешения (permit) или запрета (deny). Для удаления записи воспользуйтесь формой **no**.

Расширенный список управления доступом Expert (Extended Expert ACL):

rule [*SEQUENCE-NUMBER*] **{permit | deny}** *PROTOCOL* **{***SRC-IP-ADDR SRC-IP- WILDCARD* **| host** *SRC-IP-ADDR* **| any} {***SRC-MAC-ADDR SRC-MAC-WILDCARD* **| host** *SRC-MAC-ADDR* **|any} {***DST-IP-ADDR DST-IP-WILDCARD* **| host** *DST-IP-ADDR* **| any} {***DST-MAC-ADDR DST-MAC-WILDCARD* **| host** *DST-MAC-ADDR* **| any} [cos** *OTER-COS*] **[vlan** *OUTER-VLAN*] **[fragments] [[precedence** *PRECEDENCE*] **[tos** *TOS*] **| dscp** *DSCP*] **[time-range** *PROFILE-NAME*]

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

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

rule [*SEQUENCE-NUMBER***] {permit | deny} icmp {***SRC-IP-ADDR SRC-IP-WILDCARD* **| host** *SRC-IP-ADDR* **| any} {***SRC-MAC-ADDR SRC-MAC-WILDCARD* **| host** *SRC-MAC- ADDR* **| any} {***DST-IP-ADDR DST-IP-WILDCARD* **| host** *DST-IP-ADDR* **| any} {***DST-MAC- ADDR DST-MAC-WILDCARD* **| host** *DST-MAC-ADDR* **| any} [***ICMP-TYPE* **[***ICMP-CODE***] |** *ICMP-MESSAGE***] [cos** *OUTER-COS***] [vlan** *OUTER-VLAN***] [[precedence** *PRECEDENCE***] [tos** *TOS***] | dscp** *DSCP***] [time-range** *PROFILE-NAME***]**

no *SEQUENCE-NUMBER*

Параметры

SEQUENCE-NUMBER	Укажите порядковый номер. Доступен диапазон от 1 до 65535. Чем меньше номер, тем выше приоритет правила permit/deny.
cos *OUTER-COS*	(Опционально) Укажите значение outer priority. Доступен диапазон значений от 0 до 7.
vlan *OUTER-VLAN*	(Опционально) Укажите outer VLAN ID.
any	Укажите, чтобы использовать любой MAC-адрес источника, любой MAC-адреса назначения, любой IP-адрес источника или любой IP-адрес назначения.
host *SRC-MAC-ADDR*	Укажите конкретный MAC-адрес узла источника.
SRC-MAC-ADDR SRC-MAC-WILDCARD	Укажите группу MAC-адресов источника, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
host *DST-MAC-ADDR*	Укажите конкретный MAC-адрес узла назначения.
DST-IP-ADDR DST-IP-WILDCARD	Укажите группу MAC-адресов назначения, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
PROTOCOL	(Опционально) Укажите ID IP-протокола. Доступны следующие имена: eigrp, esp, gre, igmp, ospf, pim, vrrp, pcp и ipinip.
host *SRC-IP-ADDR*	Укажите конкретный IP-адрес узла источника.
SRC-IP-ADDR SRC-IP-WILDCARD	Укажите группу IP-адресов источника, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
host *DST-IP-ADDR*	Укажите конкретный 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.
tos *TOS*	(Опционально) Укажите, чтобы пакеты могли фильтроваться по уровню type of service. Доступны значения от 0 до 15.
dscp *DSCP*	(Опционально) Укажите DSCP-код для совпадений с заголовком IP. Доступен диапазон 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 (по умолчанию) - 000000, ef – 101110.
lt *PORT*	(Опционально) Укажите для сопоставления, если значение указанного порта меньше.

eq *PORT*	(Опционально) Укажите для сопоставления, если значение указанного порта равно.
neq *PORT*	(Опционально) Укажите для сопоставления, если значение указанного порта не равно.
range *MIN-PORT MAX-PORT*	(Опционально) Укажите для сопоставления, если значение попадает в указанный диапазон портов.
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 периода времени, связанного со списком доступа, определяющим период его активации.
ICMP-TYPE	(Опционально) Укажите тип сообщения ICMP. Доступны значения типа сообщений от 0 до 255
ICMP-CODE	(Опционально) Укажите код сообщения ICMP. Доступны значения 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, header, hop-limit, mld-query, mld-reduction, mld-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, unreachable.

По умолчанию

Нет

Режим ввода команды

Extended Expert Access-list Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если правило создано без указания определенного порядкового номера, он будет присвоен автоматически. Если это первая запись, то будет присвоен начальный порядковый номер 10. Последующим записям правила назначается номер, больший на значение шага 10; а самый большой порядковый номер в списке доступа будет стоять в конце.

Пользователь может использовать команду **access-list resequence** для смены начального порядкового номера и значения шага записей для указанного списка доступа. После применения команды новым записям без указанного порядкового номера будет задан номер в соответствии с новыми настройками указанного списка доступа.

При назначении порядкового номера вручную, лучше иметь зарезервированный интервал для будущих записей с меньшим порядковым номером. Иначе будет сложно вставить запись с еще меньшим порядковым номером.

Порядковый номер должен быть уникальным в домене списка доступа. При вводе занятого порядкового номера появится сообщение об ошибке.

Пример

В данном примере показано, как использовать расширенный список управления доступом Expert (extended expert ACL). Цель – запретить (deny) все TCP-пакеты с IP-адресом источника 192.168.4.12 и MAC-адресом источника 00:13:00:49:82:72.

```
Switch# configure terminal
Switch(config)#expert access-list extended exp_acl
Switch(config-exp-nacl)# rule deny tcp host 192.168.4.12 host 0013.0049.8272
any
Switch(config-exp-nacl)# end
Switch# show access-list expert
Extended EXPERT access list exp_acl(ID: 9998)
  10 deny TCP host 192.168.4.12 any host 00:13:00:49:82:72 any
```

4-18 permit | deny (ip access-list)

Данная команда используется для добавления записи разрешения (permit) или запрета (deny). Для удаления записи воспользуйтесь формой **no**.

Расширенный список управления доступом (Extended Access List):

rule [*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*] **{any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT*] [*TCP-FLAG*][**[precedence** *PRECEDENCE*] **[tos** *TOS*] **| dscp** *DSCP*] **[time-range** *PROFILE-NAME*]

rule [*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*] **{any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT*] **[[precedence** *PRECEDENCE*] **[tos** *TOS*] **| dscp** *DSCP*] **[time-range** *PROFILE-NAME*]

rule [*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*] **[tos** *TOS*] **| dscp** *DSCP*] **[time-range** *PROFILE-NAME*]

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

rule [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*] **[[precedence** *PRECEDENCE*] **[tos** *TOS*] **| dscp** *DSCP*] **[time-range** *PROFILE-NAME*]

Стандартный список доступа IP (Standard IP Access List):

rule [SEQUENCE-NUMBE**R**] **{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. Доступен диапазон от 1 до 65535 Чем меньше номер, тем выше приоритет правила permit/deny.
any	Укажите IP-адрес источника или IP-адрес назначения.
host *SRC-IP-ADDR*	Укажите определенный IP-адрес узла источника.
SRC-IP-ADDR SRC-IP-WILDCARD	Укажите группу IP-адресов источника, используя значение 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.
dscp *DSCP*	(Опционально) Укажите DSCP-код для совпадений с заголовком IP. Доступен диапазон 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.
tos *TOS*	(Опционально) Укажите, чтобы пакеты могли фильтроваться по уровню type of service. Доступны значения от 0 до 15
lt *PORT*	(Опционально) Укажите для сопоставления, если значение указанного порта меньше.
gt *PORT*	(Опционально) Укажите для сопоставления, если значение указанного порта больше.
eq *PORT*	(Опционально) Укажите для сопоставления, если значение указанного порта равно.
neq *PORT*	(Опционально) Укажите для сопоставления, если значение указанного порта не равно.
range *MIN-PORT MAX-PORT*	(Опционально) Укажите для сопоставления, если значение попадает в указанный диапазон портов.
time-range *PROFILE-NAME*	(Опционально) Укажите имя профиля периода времени, связанного со списком доступа, определяющим период его активации.
tcp, udp, igmp, gre, esp, eigrp, ospf, pcp, pim, vrrp	Укажите протоколы 4 уровня.
PROTOCOL-ID	(Опционально) Укажите Protocol ID. Доступен диапазон значений от 0 до 255.
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, router- 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Если правило создано без указания определенного порядкового номера, он будет присвоен автоматически. Если это первая запись, то будет присвоен начальный порядковый номер 10. Последующим записям правила назначается номер, больший на значение шага 10; а самый большой порядковый номер в списке доступа будет стоять в конце.

Пользователь может использовать команду **access-list resequence** для смены начального порядкового номера и значения шага записей для указанного списка доступа. После применения команды новым записям без указанного порядкового номера будет задан номер в соответствии с новыми настройками указанного списка доступа.
При назначении порядкового номера вручную, лучше иметь зарезервированный интервал для будущих записей с меньшим порядковым номером. Иначе будет сложно вставить запись с еще меньшим порядковым номером.

Порядковый номер должен быть уникальным в домене списка доступа. При вводе занятого порядкового номера появится сообщение об ошибке.

Для создания правила сопоставления для стандартного списка доступа IP (IP standard access list) могут быть указаны только поля IP-адреса источника и назначения.

Пример

В данном примере показано, как создать 4 записи для расширенного списка доступа IP с именем Strict-Control. Это следующие записи: разрешить TCP-пакеты, предназначенные для сети 10.20.0.0, разрешить TCP-пакеты, предназначенные 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)# rule permit tcp any 10.20.0.0 0.0.255.255
Switch(config-ip-ext-acl)# rule permit tcp any host 10.100.1.2
Switch(config-ip-ext-acl)# rule permit tcp any any eq 80
Switch(config-ip-ext-acl)# rule permit icmp any any
Switch(config-ip-ext-acl)#
```

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

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

4-19 permit | deny (ipv6 access-list)

Данная команда используется для добавления записи permit или deny в список доступа IPv6. Для удаления записи из списка доступа IPv6 воспользуйтесь формой **no**.

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**] {any | host** DST-IPV6-ADDR **|** DST-IPV6-ADDR/PREFIX-LENGTH**} [{eq | lt | gt | neq}** PORT **| range** MIN-PORT MAX-PORT**][dscp** VALUE**] [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**] {any | host** DST-IPV6-ADDR **|** DST-IPV6-ADDR/PREFIX-LENGTH**} [{eq | lt | gt | neq}** PORT **| range** MIN-PORT MAX-PORT**][dscp** VALUE**] [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**] [time-range** PROFILE-NAME**]**

[SEQUENCE-NUMBER**] {permit | deny} {protocol-id** PROTOCOL-ID**} {any | host** SRC-IPV6-ADDR **|** SRC-IPV6 ADDR/PREFIX-LENGTH**} {any | host** DST-IPV6-ADDR **|** DST-IPV6-ADDR/PREFIX-LENGTH**} [dscp** VALUE**] [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**] [dscp** VALUE**] [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. Доступен диапазон от 1 до 65535 Чем меньше номер, тем выше приоритет правила permit/deny.
any	Укажите IPv6-адрес источника или IPv6-адрес назначения.
host *SRC-IPv6-ADDR*	Укажите определенный IPv6-адрес узла источника.
SRC-IPV6-ADDR/PREFIX-LENGTH	Укажите сеть IPv6 источника.
host *DST-IPV6-ADDR*	Укажите определенный IPv6-адрес узла назначения.
DST-IPV6-ADDR/PREFIX-LENGTH	Укажите сеть IPv6 назначения.
tcp, udp, icmp, esp, pcp ,sctp	Укажите тип протокола 4 уровня.
dscp *VALUE*	(Опционально) Укажите совпадающее значение класса трафика в IPv6- хедере. Доступен диапазон 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 - 000000, ef – 101110.
lt *PORT*	(Опционально) Укажите для сопоставления, если значение указанного порта меньше.
gt *PORT*	(Опционально) Укажите для сопоставления, если значение указанного порта больше.
eq *PORT*	(Опционально) Укажите для сопоставления, если значение указанного порта равно.
neq *PORT*	(Опционально) Укажите для сопоставления, если значение указанного порта не равно.
range *MIN-PORT MAX-PORT*	(Опционально) Укажите для сопоставления, если значение попадает в указанный диапазон портов.
PROTOCOL-ID	(Опционально) Укажите Protocol ID. Доступен диапазон значений от 0 до 255.
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.
time-range *PROFILE-NAME*	(Опционально) Укажите имя профиля периода времени, связанного со списком доступа, определяющим период его активации.
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. Доступны значения от 0 до 1048575.
fragments	(Опционально) Укажите для фильтрации фрагментов пакета.

По умолчанию

Нет

Режим ввода команды

IPv6 Access-list Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если правило создано без указания определенного порядкового номера, он будет присвоен автоматически. Если это первая запись, то будет присвоен начальный порядковый номер 10. Последующим записям правила назначается номер, больший на значение шага 10; а самый большой порядковый номер в списке доступа будет стоять в конце.

Пользователь может использовать команду **access-list resequence** для смены начального порядкового номера и значения шага записей для указанного списка доступа. После применения команды новым записям без указанного порядкового номера будет задан номер в соответствии с новыми настройками указанного списка доступа.

При назначении порядкового номера вручную, лучше иметь зарезервированный интервал для будущих записей с меньшим порядковым номером. Иначе будет сложно вставить запись с еще меньшим порядковым номером.

Порядковый номер должен быть уникальным в домене списка доступа. При вводе занятого порядкового номера появится сообщение об ошибке.

Пример

В данном примере показано, как создать 4 записи для расширенного списка доступа IPv6 с именем «ipv6-control». Это следующие записи: разрешить TCP-пакеты, предназначенные для сети ff02::0:2/16, разрешить TCP-пакеты, предназначенные 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)# rule permit tcp any ff02::0:2/16
Switch(config-ipv6-ext-acl)# rule permit tcp any host ff02::1:2
Switch(config-ipv6-ext-acl)# rule permit tcp any any eq 80
Switch(config-ipv6-ext-acl)# rule permit icmp any any
Switch(config-ipv6-ext-acl)#
```

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

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

4-20 permit | deny (mac access-list)

Данная команда используется для определения правила для пакетов, которым будет разрешено или отказано в доступе. Для удаления записи воспользуйтесь формой **no**.

rule [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** TYPE MASK **[cos** VALUE **[inner** INNER-COS**]] [{vlan** VLAN-ID**} [inner** INNER-VLAN**]] [time-range** PROFILE-NAME**]**
no SEQUENCE-NUMBER

Параметры

SEQUENCE-NUMBER	Укажите порядковый номер. Доступен диапазон от 1 до 65535 Чем меньше номер, тем выше приоритет правила permit/deny.
any	Укажите MAC-адрес источника или MAC-адрес назначения.
host *SRC-MAC-ADDR*	Укажите определенный MAC-адрес узла источника.
SRC-MAC-ADDR SRC-MAC-WILDCARD	Укажите группу MAC-адресов источника, используя значение 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 тип Ethernet, являющийся шестнадцатеричным числом от 0 до FFFF или именем 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, arp.
cos *VALUE*	(Опционально) Укажите значение priority (приоритета) от 0 до 7.
vlan *VLAN-ID*	(Опционально) Укажите VLAN-ID.
time-range *PROFILE-NAME*	(Опционально) Укажите имя профиля периода времени, связанного со списком доступа, определяющим 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. Если это первая запись, то будет присвоен начальный порядковый номер 10. Последующим записям правила назначается номер, больший на значение шага 10; а самый большой порядковый номер в списке доступа будет стоять в конце.

Пользователь может использовать команду **access-list resequence** для смены начального порядкового номера и значения шага записей для указанного списка доступа. После применения команды новым записям без указанного порядкового номера будет задан номер в соответствии с новыми настройками указанного списка доступа.

При назначении порядкового номера вручную, лучше иметь зарезервированный интервал для будущих записей с меньшим порядковым номером. Иначе будет сложно вставить запись с еще меньшим порядковым номером.

Порядковый номер должен быть уникальным в домене списка доступа. При вводе занятого порядкового номера появится сообщение об ошибке.

В список может быть добавлено несколько записей, и вы можете использовать разрешение (permit) для одних, и запрет (deny) для других записей. 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)# rule permit 00:80:33:00:00:00  00:00:00:ff:ff:f
Switch(config-mac-ext-acl)# rule permit 00:f4:57:00:00:00 00:00:00:ff:ff:ff
Switch(config-mac-ext-acl)#
```

4-21 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 интерфейс, который необходимо отобразить.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Если интерфейс не указан, отображаться будет 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#
```

4-22 show access-list

Данная команда используется для просмотра информации о настройках списка доступа.

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

Параметры

ip	(Опционально) Укажите, чтобы отобразить все списки доступа IP.
mac	(Опционально) Укажите, чтобы отобразить все списки доступа MAC.
ipv6	(Опционально) Укажите, чтобы отобразить все списки доступа IPv6.
expert	(Опционально) Укажите, чтобы отобразить все списки доступа Expert.
NAME **|** *NUMBER*	Укажите имя или номер списка доступа (access list), который необходимо отобразить.
arp	Укажите, чтобы отобразить список доступа ARP.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения информации о списках доступа. Если не указана опция, будет отображен список всех настроенных списков доступа. Если указан тип списка доступа, будет отображена детальная информация о списке доступа. Если пользователь включит 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 включить отображение всех списков доступа.

```
Switch# show access-list

Access-List-Name                      Type
------------------------------------- ---------------
simple-ip-acl(ID: 3998)               ip ext-acl
simple-rd-acl(ID: 3999)               ip ext-acl
rd-mac-acl(ID: 6998)                  mac ext-acl
rd-ip-acl(ID: 1998)                   ip acl
ip6-acl(ID: 12999)                    ipv6 ext-acl
park-arp-acl                          arp acl

Total Entries: 6

Switch#
```

В данном примере показано, как включить отображение списков доступа IP с именем R&D.

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

IP access list R&D(ID:3996)
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#
```

В данном примере показано, как включить отображение содержимого списка доступа, если включен аппаратный счетчик.

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

IP access list simple-ip-acl(ID:3994)
10 permit tcp any 10.20.0.0 0.0.255.255  (Ing: 12410 packets)
20 permit tcp any host 10.100.1.2   (Ing: 6532 packets)
30 permit icmp any any   (Ing: 8758 packets)

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

Switch#
```

4-23 show vlan access-map

Данная команда используется для просмотра информации о настройках VLAN access map.

show vlan access-map [*MAP-NAME***]**

Параметры

MAP-NAME	(Опционально) Укажите имя настраиваемой VLAN access map. Имя не может содержать более 32 символов.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Если не указано имя access-map, отображаться будет вся информация о VLAN access-map. Если включен аппаратный счетчик ACL (ACL hardware counter) для access-map, отображаться будет счетчик для каждой sub-map.

Пример

В данном примере показано, как включить отображение VLAN access-map.

```
Switch# show vlan access-map

VLAN access-map vlan-map 10
  match ip access list: stp_ip1(ID: 1888)
  action: forward
VLAN access-map vlan-map 20
  match mac access list:  ext_mac(ID: 6995)
  action: redirect  eth1/0/5

Switch#
```

В данном примере показано, как включить отображение содержимого VLAN access-map, если включен аппаратный счетчик.

```
Switch# show vlan access-map

VLAN access-map vlan-map 10
  match ip access list: stp_ip1(ID: 1888)
  action: forward
    Counter enable on VLAN(s): 1-2
    match count: 8541 packets
VLAN access-map vlan-map 20
  match mac access list: ext_mac(ID: 6995)
  action: redirect eth1/0/5
    Counter enable on VLAN(s): 1-2
    match count: 5647 packets

Switch#
```

4-21 show vlan filter

Данная команда используется для просмотра информации о настройках фильтрации VLAN (VLAN filter) для интерфейсов VLAN.

show vlan filter [access-map *MAP-NAME* | **vlan** *VLAN-ID***]**

Параметры

access-map *MAP-NAME*	(Опционально) Укажите имя VLAN access-map. Имя не может содержать более 32 символов.
vlan *VLAN-ID*	(Опционально) Укажите VLAN ID.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Команда **show vlan filter access-map** используется для просмотра информации о фильтрации VLAN (VLAN filter) на основе access map. Команда **show vlan filter vlan** используется для просмотра информации о фильтрации VLAN на основе VLAN.

Пример

В данном примере показано, как включить отображение информации о фильтрации VLAN.

```
Switch# show vlan filter

VLAN Map aa
  Configured on VLANs: 5-127,221-333
VLAN Map bb
  Configured on VLANs: 1111-1222

Switch#

Switch# show vlan filter vlan 5

VLAN ID 5
  VLAN Access Map: aa

Switch#
```

4-22 vlan access-map

Данная команда используется для создания sub-map для VLAN access-map и входа в режим VLAN Access-map Sub-map Configure Mode. При использовании формы **no** команда удалит access map или ее sub-map.

vlan access-map *MAP-NAME* **[***SEQUENCE-NUM***]**
no vlan access-map MAP-NAME **[**SEQUENCE-NUM**]**

Параметры

MAP-NAME	Укажите имя VLAN access-map. Имя не может содержать более 32 символов.
SEQUENCE-NUM	(Опционально) Укажите порядковый номер sub-map. Доступен диапазон значений от 1 до 65535

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

VLAN access map может содержать несколько sub-maps. Для каждой sub-map может быть указан один список доступа (IP access list, IPv6 access list или MAC access list) и одно действие. После создания VLAN access map пользователь может использовать команду **vlan filter** для применения access map к VLAN.

Порядковый номер назначается автоматически, если пользователь не назначит его вручную. Автоматически назначенный номер начинается с 10 и увеличивается на 10 с каждой новой записью.

Пакет, совпадающий с sub-map (если пакет разрешен соответствующим списком доступа), будет действовать в соответствии с sub-map. Далее проверки sub-maps проводиться не будут. Если пакет не соответствует одной sub-map, проверяться будет следующая sub-map.

При использовании формы **no** без указаний порядковых номеров команда удалит всю информацию о sub-map указанной access map.

Пример

В данном примере показано, как создать VLAN access map.

```
Switch# configure terminal
Switch(config)# vlan access-map vlan-map 20
Switch(config-access-map)#
```

4-23 vlan filter

Данная команда используется для применения VLAN access map к VLAN. При использовании формы **no** команда удалит VLAN access map с VLAN.

vlan filter *MAP-NAME* **vlan-list** *VLAN-ID-LIST*
no vlan filter *MAP-NAME* **vlan-list** *VLAN-ID-LIST*

Параметры

MAP-NAME	Укажите имя VLAN access map.
VLAN-ID-LIST	Укажите список VLAN ID.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

С одним VLAN может быть связана только одна VLAN access map.

Пример

В данном примере показано, как применить VLAN access map «vlan-map» к VLAN 5

```
Switch# configure terminal
Switch(config)# vlan filter vlan-map vlan-list 5
Switch(config-access-map)# end
Switch# show vlan filter

VLAN Map vlan-map
  Configured on VLANs: 5

Switch#
```

---

5. Команды управления доступом

5-1 access class

Данная команда используется для указания списка, которому необходимо ограничить доступ к сессии. Для отмены проверки указанного списка доступа воспользуйтесь формой **no**.

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

Параметры

IP-ACL	Используется для указания стандартного списка доступа IP-адресов. Поле адреса источника с записью permit или deny определяет доверенный или недоверенный узел.

По умолчанию

Нет

Режим ввода команды

Line Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Данная команда указывает список, 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**.

Пример

В данном примере показан процесс создания стандартного списка доступа IP-адресов и указания на ограничение через Telnet. Только узлу 226.1.1.1 разрешен доступ к серверу.

```
Switch# configure terminal
Switch(config)#ip access-list vty-filter
Switch(config-ip-acl)#rule 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 banner login

Данная команда используется для входа в режим Banner Login Mode и настройки отображения баннера приветствия. При использовании формы **no** команда вернется к настройкам по умолчанию.

banner login *cMESSAGEc*
no banner login

Параметры

c	Разделитель текста баннера приветствия, например, знак #. Употребление символа разделителя недопустимо в тексте баннера приветствия.
MESSAGE	Содержимое баннера приветствия, отображаемое до появления окна ввода имени пользователя и пароля.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет настроить уникальный баннер, который будет отображаться после успешного входа пользователя в систему. После команды banner login поставьте как минимум один пробел и любой разделитель на выбор. Далее введите одну или более строку текста, закончив сообщение вторым разделителем.

Например, если разделителем является символ «#», то после его ввода нужно нажать клавишу Enter и ввести содержимое баннера входа. Далее необходимо снова ввести разделитель и нажать Enter для завершения. Чтобы вернуться к содержимому баннера входа по умолчанию используйте форму **no** в режиме глобальной конфигурации.

Примечание: все дополнительные символы, введенные после последнего разделителя, будут недействительны и будут отброшены. Символ разделитель нельзя использовать в тексте баннера приветствия.

Пример

В данном примере показан процесс настройки сообщения баннера приветствия. Символ «#» является разделителем. Первый разделитель содержимого баннера и последний разделитель необходимо ввести до первого нажатия клавиши Enter.

```
Switch# configure terminal
Switch(config)# banner login #Enter Command Line Interface#
Switch(config)#
```

В данном примере показан процесс настройки сообщения баннера приветствия. Символ «#» является разделителем. Только первый разделитель вводится до первого нажатия клавиши Enter.

```
Switch# configure terminal
Switch(config)# banner login #
LINE  c banner-text c, where 'c' is a delimiting character
Enter Command Line Interface
#
Switch(config)#
```

5-3 do

Эта команда используется для выполнения команд, изначально находящихся в режиме User/Privileged EXEC в любом режиме конфигурации.

do *COMMAND*

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Любой режим конфигурации

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для выполнения команд, изначально находившихся в режиме User/Privileged EXEC, таких как **show**, **clear** или **debug**, во время конфигурирования коммутатора. После выполнения команды система вернется в режим конфигурирования, который вы использовали.

Примечание: вопросительный знак (?) и клавиша Tab доступны для команды **do**

Пример

В этом примере показано, как использовать вопросительный знак (?) с этой командой.

```
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)#
```

В этом примере показано, как выполнить команду show running-config в режиме глобальной конфигурации.

```
Switch#configure terminal
Switch(config)#do show running-config
Building configuration...

Current configuration : 1467 bytes

!-----------------------------------------------------------------------------
!                DGS-1510-28XMP Gigabit Ethernet SmartPro Switch
!                                Configuration
!
!                            Firmware: Build 1.70.005
!           Copyright(C) 2020 D-Link Corporation. All rights reserved.
!-----------------------------------------------------------------------------

line console
!
line telnet
!
line ssh
!
ssh user admin authentication-method password
!
no ip domain lookup
ip name-server timeout 3
!
interface ethernet 1/0/1
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

5-4 prompt

Данная команда используется для настройки определенной командной строки. При использовании формы **no** команда вернется к настройкам по умолчанию

prompt *STRING*
no prompt

Параметры

STRING	Строка для определения настраиваемой подсказки. Подсказка будет основываться на определенных символах или следующих символах управления. Пробел в строке игнорируется. **%h** – шифрование имени сервера SNMP **%s** – пробел **%%** – шифрование символа %

По умолчанию

По умолчанию строка шифрует имя сервера SNMP.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет настроить подсказку командной строки. Если пользователь выберет шифрование имени сервера SNMP в качестве подсказки, зашифрованы будут только первые 15 символов. Подсказка может отобразить только 15 символов. Символ уровня привилегии будет отображаться последним символом подсказки.
Символы определяются по следующим правилам:
> – уровень пользователя
– уровень привилегии пользователя

Пример

В данном примере показан процесс настройки подсказки «BRANCH A», используя учетную запись администратора.

```
Switch# configure terminal
Switch(config)# prompt BRANCH%sA
BRANCH A(config)#
```

В этом примере показано, как вернуть командный интерпретатор к настройкам по умолчанию.

```
BRANCH A#configure terminal
BRANCH A(config)#no prompt
Switch(config)#
```

5-5 enable password

Данная команда позволяет включить ввод пароля для входа на различные уровни привилегии. При использовании формы **no** команда вернет пароль к пустому значению.

enable password [level *PRIVILEGE-LEVEL***] [0 | 7 | 15]** *PASSWORD*
no enable password [level *PRIVILEGE-LEVEL***]**

Параметры

level PRIVILEGE-LEVEL	(Опционально) Указывает уровень привилегии для пользователя. Диапазон доступных уровней привилегий: от 1 до 15 Если это значение не введено, или используется форма no, уровнем по умолчанию считается 15.
0	(Опционально) Пароль в обычном текстовом виде. Длина пароля может составлять от 1 до 32 символов и содержать пробелы. Пароль чувствителен к регистру. Если синтаксис пароля не указан, им будет простой текст.
7	(Опционально) Зашифрованный пароль на основе SHA-1. Длина пароля ограничена 35 байтами. Пароль чувствителен к регистру и зашифрован. Если синтаксис пароля не указан, им будет простой текст.
15	(Опционально) Зашифрованный пароль на основе MD5. Длина пароля ограничена 31 байтом. Пароль чувствителен к регистру и зашифрован. Если синтаксис пароля не указан, им будет простой текст.
PASSWORD	Пароль для использования.

По умолчанию

По умолчанию пароль не задан. Данная строка остается пустой.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Назначение пароля для входа на различные уровни привилегии. Каждый уровень имеет только один пароль.

Пример

В данном примере показан процесс назначения пароля «MyEnablePassword» для уровня привилегии 15.

```
Switch# configure terminal
Switch(config) #enable password MyEnablePassword
Switch# disable
Switch# enable
Password:***************
Switch# show privilege
Current privilege level is 15
Switch#
```

5-6 ip http server

Данная команда позволяет включить сервер HTTP. При использовании формы no команда отключит сервер HTTP.

ip http server
no ip http server

Параметры

Нет

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет включить сервер HTTP. Интерфейс доступа HTTPS отдельно управляется командами SSL.

Пример

В данном примере показан процесс включения сервера HTTP.

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

5-7 ip http secure-server

Эта команда используется для включения сервера HTTPS. Используйте команду **ip http secure-server ssl-service- policy**, чтобы указать, какая политика службы SSL используется для HTTPS. Используйте форму no этой команды, чтобы отключить функцию сервера HTTPS.

ip http secure-server [ssl-service-policy *POLICY-NAME*]
no ip http secure-server

Параметры

POLICY-NAME	Указывает имя политики службы SSL. Используйте это ключевое слово **ssl- service-policy**, только если вы уже объявили политику службы SSL с помощью команды **ssl-service-policy**. Если ключевое слово не указано, для HTTPS будет использоваться встроенный локальный сертификат.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда включает функцию сервера HTTPS и использует указанную политику службы SSL для HTTPS.
Пример

В этом примере показано, как включить функцию сервера HTTPS и использовать политику обслуживания под названием "sp1" для HTTPS.

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

5-8 ip {http | https} access-class

Эта команда используется для указания списка доступа для ограничения доступа к серверу HTTP или HTTPs. Используйте форму **no** этой команды, чтобы удалить проверку списка доступа.

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

Параметры

IP-ACL	Определяет стандартный список доступа IP. Поле адреса источника записи определяет допустимый или недопустимый хост.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда определяет список доступа для ограничения доступа к серверу HTTP или HTTPs. Если указанный список доступа не существует, команда не вступает в силу, поэтому список доступа не проверяется для доступа пользователя к HTTP или HTTPs.

Пример

В этом примере показано, как создается стандартный список доступа IP и указывается в качестве списка доступа для доступа к HTTP-серверу. Доступ к серверу разрешен только хосту 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)#
```

5-9 ip http service-port

Эта команда используется для указания порта службы HTTP. Используйте форму **no** этой команды, чтобы вернуть служебный порт на значение 80.

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

Параметры

TCP-PORT	Номер порта TCP. Диапазон портов TCP: 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет указать TCP-порт для сервера HTTP.

Пример

В данном примере показан процесс настройки TCP-порта 8080 для HTTP.

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

5-10 ip http timeout-policy idle

Данная команда позволяет задать значение тайм-аута для подключения к серверу HTTP. При использовании формы **no** команда вернется к настройкам по умолчанию.

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

Параметры

INT	Значение таймера в секундах. Допустимый диапазон: от 60 до 36000

По умолчанию

По умолчанию значение составляет 180 секунд.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет задать значение тайм-аута для подключения к серверу HTTP.

Пример

В данном примере показан процесс настройки тайм-аута со значением 100 секунд.

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

5-11 ip telnet server

Данная команда используется для включения сервера Telnet. При использовании формы **no** команда отключит сервер Telnet.

ip telnet server
no ip telnet server

Параметры

Нет

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

В данном примере показан процесс включения сервера Telnet.

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

5-12 ip telnet service port

Данная команда позволяет задать порт для Telnet. При использовании формы **no** команда вернется к настройкам по умолчанию.

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

Параметры

TCP-PORT	Номер порта TCP. Диапазон портов TCP: 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет указать TCP-порт для доступа к Telnet.

Пример

В данном примере показан процесс настройки сервисного порта 3000 для Telnet.

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

5-13 line

Данная команда позволяет идентифицировать тип сессии для конфигурации и войти в режим Line Configuration Mode.

line {console | telnet | ssh}

Параметры

console	Локальная консольная сессия терминала.
telnet	Сессия терминала Telnet.
ssh	Сессия терминала SSH.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет войти в режим Line Configuration Mode.

Пример

В данном примере показан процесс входа в режим Line Configuration Mode для сессии терминала SSH и настройки класса доступа «vty-filter».

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

5-14 service password-encryption

Данная команда используется для включения шифрования пароля перед сохранением в файле конфигурации. При использовании формы **no** команда отключит шифрование.

service password-encryption [7 | 15]
no service password-encryption

Параметры

7	(Опционально) Пароль, зашифрованный на основе SHA-1.
15	(Опционально) Пароль, зашифрованный на основе MD5.

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Информация о конфигурации учетной записи пользователя хранится в текущем файле конфигурации (running configuration) и может применяться позднее. Если включена команда **service password-encryption**, пароль будет храниться в зашифрованном виде.

Если опция шифрования пароля отключена, а пароль указан в простой текстовой форме, он сохранится в форме обычного текста. Но если пароль указан в зашифрованном виде или пароль был преобразован в зашифрованную форму командой **service password-encryption**, пароль будет храниться в зашифрованном виде. Его нельзя будет перевести обратно в простую текстовую форму.

Данная команда применяется к паролю учетной записи пользователя, заданному паролю и паролю аутентификации.

Пример

В данном примере показан процесс включения шифрования пароля перед сохранением в файле конфигурации.

```
Switch# configure terminal
Switch(config)# service password-encryption
Switch(config)#
```

5-15 show terminal

Данная команда используется для получения информации о настройках параметров конфигурации терминала для текущей сессии терминала.

show terminal

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для получения информации о настройках терминала для текущей сессии.

Пример

В данном примере показан процесс отображения информации 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: 9600 bps

Switch#
```

5-16 show ip http server

Эта команда используется для получения информации о состоянии сервера Telnet. Используйте эту команду в любом пользовательском/привилегированном режиме EXEC.

show ip http server

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень1

Использование команды

Используйте эту команду для отображения информации о состоянии сервера Telnet.

Пример

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

```
Switch# show ip telnet server

Server State: Enabled

Switch#
```

5-17 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

В данном примере показан процесс отображения информации о состоянии HTTP-сервера.

```
Switch# show ip http server

ip http server state :  enable

Switch#
```

5-18 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения информации о состоянии SSL.

Пример

В данном примере показан процесс отображения информации о состоянии SSL.

```
Switch# show ip http secure-server

ip http secure-server state :  disable

Switch#
```

5-19 show users

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

show users

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

В данном примере показан процесс отображения информации обо всех сессиях.

```
Switch# show users
ID   Type      User-Name       Privilege Login-Time          IP address
------------------------------------------------------------------------------
0    * console admin           15        4S

Total Entries: 1

Switch#
```

5-20 telnet

Данная команда позволяет подключиться к другому устройству с поддержкой Telnet.

telnet [*IP-ADDRESS* | *IPV6-ADDRESS* I *Domain-Name*] [*TCP-PORT*]

Параметры

IP-ADDRESS	IPv4-адрес узла.
IPV6-ADDRESS	IPv6-адрес узла.
Domain-Name	Указывает имя узла назначения Telnet.
TCP-PORT	Номер порта TCP. Диапазон портов TCP: от 1 до 65535 Как правило, для Telnet назначается TCP-порт 23

По умолчанию

Нет

Режим ввода команды

EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Это функция клиента Telnet, которую можно использовать для связи с другим устройством с помощью функции Telnet. В системе коммутатора может быть открыто несколько сеансов Telnet, и для каждого

открытого сеанса Telnet может одновременно поддерживаться собственное программное обеспечение клиента Telnet.

Пример

В данном примере показан процесс подключения к IP-адресу 10.90.90.91 с помощью порта 23. IP-адрес 10.90.90.91 является интерфейсом управления ТГК-313-24/6Д-М, позволяющим пользователю войти в учетную запись.

```
Switch# telnet 10.90.90.91

                    DGS-3130-30TS Gigabit Ethernet Switch

                            Command Line Interface
                           Firmware: Build 1.00.001
          Copyright(C) 2017 D-Link Corporation. All rights reserved.

Password required, but none set

Switch#
```

В данном примере показан процесс подключения по Telnet к IP-адресу 10.90.90.91 через порт 23, если подключение не удалось. Попытаемся использовать порт 3500 для входа в интерфейс управления.

```
Switch#telnet 10.90.90.91

ERROR: Could not open a connection to host on server port 23.

Switch# telnet 10.90.90.91 3500

                    DGS-3130-30TS Gigabit Ethernet Switch

                            Command Line Interface
                           Firmware: Build 1.00.001
          Copyright(C) 2017 D-Link Corporation. All rights reserved.

Password required, but none set

Switch#
```

5-21 terminal length

Данная команда используется для настройки количества строк, отображаемых на экране. Команда **terminal length** влияет только на текущую сессию. Команда **terminal default length** установит значение по умолчанию, но не повлияет на текущую сессию. Созданный заново терминал будет использовать значение по умолчанию. При использовании формы **no** команда вернет настройки поумолчанию.

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

Параметры

NUMBER	Количество строк, отображаемое на экране. Допустимы

	значения 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

User/Privileged EXEC Mode для команды **terminal length**
Global Configuration Mode для команды **terminal length default**

Уровень команды по умолчанию

Уровень 1 (для команды **terminal length**)
Уровень 12 (для команды **terminal length default**)

Использование команды

При значении 0 отображение не прекратится, пока не будет достигнут конец отображаемогоматериала.

Если для terminal length указано значение, отличное от 0, например 50, то отображение будет останавливаться после каждых 50 строк. Данная команда используется для настройки количествастрок, отображаемых на экране во время текущей сессии. Данная команда также применяется для сессий Telnet и SSH. Доступны значения от 0 до 512. Значение по умолчанию – 24. При выборе 0 коммутатор будет прокручивать информацию автоматически, без пауз.

За выводом от одной команды, выходящей за границу дисплея, будет следовать подсказка **–More–.** При появлении подсказки **–More–**, нажмите CTRL+C, q, Q или ESC, чтобы прервать вывод и вернутьсяк подсказке. 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 на 24.

Команда terminal length default доступна в режиме глобальной конфигурации Global ConfigurationMode. 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 показан процесс изменения количества строк на 60.

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

5-22 terminal speed

Данная команда используется для настройки скорости терминала. При использовании формы **no** команда вернется к настройкам по умолчанию.

terminal speed *BPS*
no terminal speed

Параметры

BPS	Скорость консоли в бит/с.

По умолчанию

Значение по умолчанию – 115200.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

В данном примере показан процесс изменения скорости последовательного порта на 9600 бит/с.

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

5-23 session-timeout

Данная команда позволяет задать значение тайм-аута сессии. При использовании формы **no** команда вернется к настройкам по умолчанию.

session-timeout *MINUTES*
no session-timeout

Параметры

MINUTES	Тайм-аут в минутах. При использовании значения 0 тайм-аут не истекаетникогда.

По умолчанию

Значение по умолчанию – 3 минуты.

Режим ввода команды

Line Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет задать значение тайм-аута сессии, после которого произойдет автоматический выход из учетной записи.

Пример

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

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

5-24 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.
Созданный заново терминал будет использовать значение по умолчанию. При использовании формы **no** команда вернется в настройки по умолчанию.

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

Параметры

NUMBER	Количество символов, отображаемое на экране. Допустимы значения от 40 до 255.

По умолчанию

Значение по умолчанию – 80.

Режим ввода команды

User/Privileged EXEC Mode для команды **terminal width**
Global Configuration Mode для команды **terminal width default**

Уровень команды по умолчанию

Уровень 1 (для команды **terminal width**)
Уровень 12 (для команды **terminal width default**)

Использование команды

По умолчанию ширина терминала составляет 80 символов. Команда **terminal width** позволяет изменить ширину терминала и применяется только к текущей сессии. При использовании формы no команда вернет значение по умолчанию, то есть 80 символов.

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

Но при удаленном доступе к сессии CLI, например, Telnet, ширина терминала автосогласования будет иметь преимущество над настройками по умолчанию, если автосогласование будет успешным. В противном случае применяться будут настройки по умолчанию.

Пример

В данном примере показан процесс изменения текущей ширины терминала на 120.

```
Switch# show terminal

Length: 24 lines
Width: 80 columns
Default Length: 24 lines
Default Width: 80 columns
Baud rate: 9600

Switch# terminal width 120
Switch# show terminal

Length: 24 lines
Width: 120 columns
Default Length: 24 lines
Default Width: 80 columns
Baud rate: 9600

Switch #
```

5-25 username

Данная команда позволяет создать учетную запись пользователя. При использовании формы **no** команда удалит учетную запись пользователя.

username *NAME* **[privilege** *LEVEL***] [nopassword | password [0 | 7 | 15]** *PASSWORD***]**
no username [*NAME***]**

Параметры

NAME	Имя пользователя, максимум 32 символа.
privilege *LEVEL*	(Опционально) Уровень привилегии для каждого пользователя. Диапазон доступных уровней: от 1 до 15.
nopassword	(Опционально) Указывает, что к данной учетной записи не будет применяться пароль.
password	(Опционально) Указывает, что к данной учетной записи будет применяться пароль.
0	(Опционально) Пароль в обычном текстовом виде. Длина пароля может составлять от 1 до 32 символов и содержать пробелы. Пароль чувствителен к регистру. Если синтаксис пароля не может быть указан, им будет обычный текст.
7	(Опционально) Пароль, зашифрованный на основе SHA-1.

	Длина пароля ограничена 35 байтами. Пароль чувствителен к регистру. Пароль зашифрован. Если синтаксис пароля не указан, им будет обычный текст.
15	(Опционально) Пароль, зашифрованный на основе MD5. Длина пароля ограничена 31 байтом. Пароль чувствителен к регистру. Пароль зашифрован. Если синтаксис пароля не указан, им будет обычный текст.
PASSWORD	(Опционально) Пароль на основе одного из указанных выше параметров.

По умолчанию

По умолчанию используется система аутентификации без имени учетной записи. Если не указано другое, используйте 1.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Данная команда позволяет создать учетную запись пользователя с различными уровнями доступа. Если пользователь входит с уровнем 1, он будет в режиме User EXEC Mode, и ему будет необходимо использовать команду **enable** для входа в режим Privileged EXEC Mode.

Если пользователь входит с уровнем 2 или выше, он сразу будет в режиме Privileged EXEC Mode. В этом режиме находятся все уровни от 2 до 15.

Пользователь может указать пароль в зашифрованной форме или в виде обычного текста. Если он в виде обычного текста, но включена функция шифрования пароля, то пароль будет изменен на зашифрованный.

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

По умолчанию учетная запись пользователя пустая. Если учетная запись пользователя пустая, ему будет сразу назначен режим User EXEC Mode и уровень 1. Пользователь может дополнительно войти в режим Privileged EXEC Mode с помощью команды **enable**.

Пример

В данном примере показан процесс создания учетной записи администратора с именем admin и паролем «mypassword».

```
Switch# configure terminal
Switch(config)# username admin privilege 15 password 0 mypassword
Switch(config)#
```

В данном примере показан процесс удаления учетной записи администратора с именем **admin**.

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

5-26 password

Данная команда позволяет создать новый пароль. При использовании формы **no** команда удалит пароль.

password [0 | 7 | 15] *PASSWORD*
no password

Параметры

0	(Опционально) Пароль в обычном текстовом виде. Длина пароля может составлять от 1 до 32 символов и содержать пробелы. Пароль чувствителен к регистру. Если синтаксис пароля не указан, им будет обычный текст.
7	(Опционально) Пароль, зашифрованный на основе SHA-1. Длина пароля ограничена 35 байтами. Пароль чувствителен к регистру. Пароль зашифрован. Если синтаксис пароля не указан, им будет обычный текст.
15	(Опционально) Пароль, зашифрованный на основе MD5. Длина пароля составляет 31 байт. Пароль чувствителен к регистру. Пароль зашифрован. Если синтаксис пароля не указан, им будет обычный текст.
PASSWORD	Пароль для пользователя

По умолчанию

Нет

Режим ввода команды

Line Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Данная команда позволяет создать новый пароль для пользователя. Для каждого типа сессии может использоваться только один пароль.

Пример

В данном примере показан процесс создания пароля для сессии консоли.

```
Switch# configure terminal
Switch(config)# line console
Switch(config-line)# password 123
Switch(config-line)#
```

5-27 clear line

Данная команда используется для завершения сессии подключения.

clear line *LINE-ID*

Параметры

LINE-ID	Указывает идентификатор линии для разрыва сеанса связи. Значение от 1 до 22.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Эта команда используется для отключения активной сессии на коммутаторе.

Пример

В данном примере показан процесс отключения сессии 1.

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

5-28 banner exec

Эта команда используется для настройки баннера, который будет отображаться при запуске процесса EXEC. Используйте форму no этой команды для удаления существующего баннера EXEC.

banner exec *cMESSAGEc*
no banner exec

Параметры

c	Указывает разделитель сообщения баннера EXEC, например, знак фунта (#). Символ-разделитель не допускается в сообщении баннера входа в систему.
MESSAGE	Указывает содержимое баннера EXEC, который будет отображаться после имени пользователя и пароля, но перед режимом EXEC.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для настройки настраиваемого баннера, который будет отображаться перед приглашением режима EXEC.

Настроенный баннер позволяет использовать определенные маркеры в виде $ в тексте сообщения для отображения текущей конфигурации или информации в Системе.

- $(hostname) - Строка, которая используется для определения сообщения подсказки.
- $(line) - Отображение идентификатора линии (идентификатора сеанса подключения).

Пример

В этом примере показано, как настроить баннер EXEC. Знак маркера ($) заменяется соответствующей конфигурацией.

```
Switch(config)#banner exec #
Enter TEXT message.  End with the character '#'.
Session established on $(hostname)#
Switch(config)#
```

5-29 exec-banner

Эта команда используется для отображения баннера EXEC на указанной строке или строках. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

exec-banner
no exec-banner

Параметры

Нет

По умолчанию

По умолчанию эта функция включена для всех линий.

Режим ввода команды

Line Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда определяет, будет ли коммутатор отображать баннер EXEC при создании сеанса EXEC.

Пример

В этом примере показано, как настроить, чтобы баннер EXEC не отображался на линии SSH.

```
Switch#configure terminal
Switch(config)#line ssh
Switch(config-line)#no exec-banner
Switch(config-line)#
```

5-30 outgoing-session-timeout

Эта команда используется для настройки значения тайм-аута исходящего сеанса. Используйте форму **no** этой команды
для возврата к настройкам по умолчанию.

outgoing-session-timeout *MINUTES*
no outgoing-session-timeout

Параметры

MINUTES	Указывает длительность тайм-аута в минутах. 0 означает "никогда". Значение от 0 до 1439.

По умолчанию

По умолчанию это значение равно 0

Режим ввода команды

Line Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для настройки значения таймаута исходящей сессии, используемого для таймаута исходящих соединений Telnet через CLI коммутатора с другим устройством.

Если таймаут происходит через виртуальное линейное соединение (соединение Telnet/SSH с коммутатором), сессия будет возвращена к приглашению Privileged EXEC Mode.

Когда таймаут происходит через физическое линейное соединение (консольное соединение с коммутатором), сессия будет выведена из системы, а линейное соединение будет возвращено в состояние ожидания.

Функция таймаута исходящей сессии имеет более высокий приоритет, чем функция таймаута сессии (подключение к коммутатору), настроенная с помощью команды session-timeout. Это означает, что локальная сессия не может быть закрыта, если исходящая сессия еще жива.

Пример

В этом примере показано, как настроить значение таймаута исходящей сессии для линии SSH.

```
Switch#configure terminal
Switch(config)#line ssh
Switch(config-line)#outgoing-session-timeout 5
Switch(config-line)#
```

5-31 terminal monitor

Команда используется для включения отладки и сообщений системного журнала для текущих сеансов Telnet/SSH. Для отключения этой функции используйте форму no этой команды.

terminal monitor
no terminal monitor

Параметры

Нет

По умолчанию

По умолчанию эта опция отключена.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для включения или отключения отладки и сообщений системного журнала для текущих сеансов Telnet/SSH.

Пример

В этом примере показано, как включить отладку и сообщения системного журнала для текущих сеансов Telnet/SSH.

```
Switch#terminal monitor
Switch#
```

6. Команды предотвращения атак ARP Spoofing

6-1 ip arp spoofing-prevention

Команда используется для настройки записи ARP Spoofing Prevention (ASP), используемой для предотвращения атак ARP. Используйте форму no, чтобы удалить запись ARP Spoofing Prevention.

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

Параметры

GATEWAY-IP	IP-адрес шлюза.
GATEWAY-MAC	MAC-адрес шлюза. Настройки MAC-адреса заменят последнюю конфигурацию для того же IP-адреса шлюза.
INTERFACE-ID	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 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки записи ARP Spoofing Prevention (ASP), чтобы предотвратить спуфинг MAC адреса защищенного шлюза. При создании записи ARP-пакеты, у которых IP-адрес их источника совпадает с IP-адресом шлюза, а MAC-адрес их источника не совпадает с MAC-адресом шлюза, будут отбрасываться. ASP будет игнорировать ARP-пакеты, если IP-адрес их 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 'trusted' или 'untrusted'.

Указать можно только физические порты.

Пример

В этом примере показано, как настроить запись предотвращения спуфинга ARP с IP-адресом 10.254.254.251 и MAC-адресом 00-00-00-11-11-11 и активировать эту запись на порту eth1/0/10 и канале порта 3.

```
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 ip arp spoofing-prevention logging enable

Эта команда используется для включения регистрации информации об атаке, когда IP-адрес атаки совпадает со шлюзом. Для отключения этой функции используйте форму **no** этой команды.

ip arp spoofing-prevention logging enable
no ip arp spoofing-prevention logging enable

Параметры

Нет

По умолчанию

По умолчанию эта опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для включения или отключения регистрации информации об атаке, когда IP-адрес атаки совпадает со шлюзом.

Пример

В этом примере показано, как включить регистрацию информации об атаке, когда IP-адрес атаки совпадает со шлюзом.

```
Switch#configure terminal
Switch(config)#ip arp spoofing-prevention logging enable
Switch(config)#
```

6-3 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

User EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения всех записей ARP Spoofing Prevention.

Пример

В данном примере показано, как включить отображение всех записей 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 запуска функции Asymmetric VLAN. Используйте форму **no**, чтобы отключить данную функцию.

asymmetric-vlan
no asymmetric-vlan

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для включения или отключения функции асимметричной сети VLAN.

Пример

В данном примере показано, как запустить функцию Asymmetric VLAN.

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

В этом 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 accounting commands

Данная команда используется для настройки списка методов аккаунтинга, используемого для всех команд на указанном уровне прав доступа. Используйте форму **no** для удаления списка методов аккаунтинга.

aaa accounting commands *LEVEL* **{default |** *LIST-NAME***} start-stop** *METHOD1* **[***METHOD2***...]**
no aaa accounting commands *LEVEL* **{default /** *LIST-NAME***}**

Параметры

LEVEL	Указывает выполнять учет для всех команд **configure** на указанном уровне прав доступа. Допустимые уровни привилегий прав доступа: от 1 до 15.
default	Указывает на настройку списка методов аккаунтинга по умолчанию.
LIST-NAME	Имя списка методов. Длина имени не должна превышать 32 символов.
start-stop	Указывает на отправку сообщений об учете при запуске и завершении процесса. Пользователям разрешается доступ к сети, независимо от того, было ли получено сообщение о начале учета сервером учета или нет.
METHOD1 [METHOD2...]	Укажите список методов, которые необходимо выполнить алгоритму аккаунтинга в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для указания метода. **group tacacs+** – указывает на использование серверов, определенныхкомандой TACACS+ server host. **group** *GROUP-NAME* – указывает на использование групп серверов, определенных командой **aaa group server tacacs+**. **none** – не выполнять аккаунтинг.

По умолчанию

Метод аккаунтинга AAA не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для настройки списка методов аккаунтинга.

Пример

В данном примере показано, как создать список методов аккаунтинга для уровня прав доступа 15, используя TACACS+, который будет отправлять accounting-сообщения в начальное и конечное время доступа.

```
Switch#configure terminal
Switch(config)# aaa accounting commands 15 list-1 start-stop group tacacs+
Switch(config)#
```

8-2 aaa accounting exec

Данная команда используется для настройки списка методов аккаунтинга, используемого EXEC для конкретной линии. Используйте форму **no** для отключения аккаунтинга EXEC.

aaa accounting exec {default | *LIST-NAME***} start-stop** *METHOD1* **[***METHOD2***...I none]**
no aaa accounting exec {default | *LIST-NAME***}**

Параметры

default	Указывает на настройку списка методов аккаунтинга по умолчанию для EXEC.
LIST-NAME	Имя списка методов. Длина имени не должна превышать 32 символов.
start-stop	Указывает на отправку сообщений об учете при запуске и завершении процесса. Пользователям разрешается доступ к сети, независимо от того, было ли получено сообщение о начале учета сервером учета или нет.
METHOD1 [METHOD2...]	Укажите список методов, которые необходимо выполнить алгоритму аккаунтинга в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могутиспользоваться для указания метода. **group radius** – указывает на использование серверов, определенных командой RADIUS server host. **group tacacs+** – указывает на использование серверов, определенных командой TACACS+ server host. **group** *GROUP-NAME* – указывает на использование групп серверов, определенных командой AAA group server. **none** – не выполнять аккаунтинг.

По умолчанию

Метод аккаунтинга AAA не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для настройки списка методов аккаунтинга EXEC.

Пример

В данном примере показано, как создать список методов аккаунтинга действий пользователей, используя RADIUS, который будет отправлять accounting-сообщения в начальное и конечное время доступа.

```
Switch#configure terminal
Switch(config)# aaa accounting exec list-1 start-stop group radius
Switch(config)#
```

8-3 aaa accounting network

Данная команда используется для аккаунтинга действий пользователей при получении доступа к сети. Используйте форму **no** для удаления списка методов аккаунтинга.

aaa accounting network default start-stop *METHOD1* **[***METHOD2***...]**
no aaa accounting network default

Параметры

network	Укажите для выполнения аккаунтинга сервисных запросов, касающихся сети.
start-stop	Указывает на отправку accounting-сообщений как в начальное, так и в конечное время доступа. Пользователям разрешен доступ к сети независимо от того, успешно ли будет включено начальное accounting- сообщение аккаунтинга.
default	Указывает на настройку списка методов аккаунтинга по умолчанию для сетевых ресурсов.
METHOD1 [METHOD2...]	Укажите список методов, которые необходимо выполнить алгоритму аккаунтинга в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для указания метода. **group radius** – указывает на использование серверов, определенныхкомандой RADIUS server host. **group tacacs+** – указывает на использование серверов, определенныхкомандой TACACS+ server host. **group** *GROUP-NAME* – указывает на использование групп серверов,определенных командой AAA group server. **none** – не выполнять аккаунтинг.

По умолчанию

Метод аккаунтинга AAA не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для настройки списка методов аккаунтинга для платы за обеспечение доступа к сети. Чтобы список методов по умолчанию вступил в силу, сначала включите AAA, используя команду **aaa new-model**. Система аккаунтинга выключена, если список методов по умолчанию не настроен.

Пример

В данном примере показано, как включить аккаунтинг платы за обеспечение доступа к сети, используя RADIUS, который будет отправлять accounting-сообщения в начальное и конечное время доступа.

```
Switch#configure terminal
Switch(config)# aaa accounting network default start-stop group radius
Switch(config)#
```

8-4 aaa accounting system

Данная команда используется для аккаунтинга событий системы. Используйте форму **no** для удаления списка методов аккаунтинга.

aaa accounting system default start-stop *METHOD1* **[***METHOD2***...]**
no aaa accounting system default

Параметры

system	Указывает на выполнение аккаунтинга событий системного уровня.
default	Указывает на настройку списка методов по умолчанию для аккаунтинга системных ресурсов.
start-stop	Указывает на отправку accounting-сообщений как в начальное, так и в конечное время доступа. Пользователям разрешен доступ к сети независимо от того, успешно ли будет включено начальное accounting- сообщение аккаунтинга
METHOD1 [METHOD2...]	Укажите список методов, которые необходимо выполнить алгоритму аккаунтинга в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для указания метода. **group radius** – указывает на использование серверов, определенныхкомандой RADIUS server host. **group tacacs+** – указывает на использование серверов, определенныхкомандой TACACS+ server host. **group** *GROUP-NAME* – указывает на использование групп серверов,определенных командой AAA group server. **none** – не выполнять аккаунтинг.

По умолчанию

Метод аккаунтинга AAA не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для настройки списка методов аккаунтинга для событий системы, таких как перезагрузка, восстановление заводских настроек по умолчанию и т. п. Чтобы список методов по умолчанию вступил в силу, сначала включите AAA, используя команду **aaa new-model**. Система аккаунтинга выключена, если список методов по умолчанию не настроен.

Пример

В данном примере показано, как включить аккаунтинг событий системы, используя RADIUS, который будет отправлять accounting-сообщения.

```
Switch#configure terminal
Switch(config)# aaa accounting system default start-stop group radius
Switch(config)#
```

8-5 aaa authentication enable

Данная команда используется для настройки списка методов по умолчанию для определения доступа к привилегированному уровню EXEC. Используйте форму **no** для удаления списка методов по умолчанию.

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

Параметры

METHOD1 [METHOD2...]	Укажите список методов, которые необходимо выполнить алгоритму аккаунтинга в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для указания метода. **enable** – указывает на использование локального пароля для аутентификации. **group radius** – указывает на использование серверов, определенных командой RADIUS server host. **group tacacs+** – указывает на использование серверов, определенных командой TACACS+ server host. **group** *GROUP-NAME* – указывает на использование групп серверов,определенных командой AAA group server. **none** – обычно метод занимает в списке последнее место. Пользователь пройдет аутентификацию, если

	это не запрещено ему предыдущим методом аутентификации.

По умолчанию

Метод аутентификации AAA не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для настройки списка методов аутентификации по умолчанию для определения доступа к привилегированному уровню EXEC, когда пользователи вводят команду **enable [privilege** *LEVEL***]**. Аутентификация с использованием RADIUS-сервера будет основана на уровне прав доступа и будет использовать «enable12» или «enable15» в качестве имени пользователя.

Пример

В данном примере показано, как установить список методов по умолчанию для аутентификации. Метод работает с группой серверов «group2».

```
Switch#configure terminal
Switch(config)# aaa authentication enable default group group2
Switch(config)#
```

8-6 aaa authentication dot1x

Данная команда используется для настройки списка методов по умолчанию, используемого для аутентификации 802.1X. Используйте форму **no** для удаления списка методов по умолчанию.

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

Параметры

METHOD1 ***[****METHOD2****...]***	Укажите список методов, которые необходимо выполнить алгоритму аккаунтинга в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для указания метода. **local** – указывает на использование локальной базы данных для аутентификации. **group radius** – указывает на использование серверов, определенных командой RADIUS server host. **group** *GROUP-NAME* – указывает на использование групп серверов,определенных командой AAA group server.

	none – обычно метод занимает в списке последнее место. Пользователь пройдет аутентификацию, если это не запрещено ему предыдущим методом аутентификации.

По умолчанию

Метод аутентификации AAA не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для настройки списка методов аутентификации 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)#
```

8-7 aaa authentication jwac

Эта команда используется для настройки списка методов по умолчанию, используемых для аутентификации JWAC. Используйте команду **no** для удаления списка методов по умолчанию.

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

Параметры

METHOD1 [METHOD2...]	Укажите список методов, которые необходимо выполнить алгоритму аккаунтинга в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для указания метода. **local** – указывает на использование локальной базы данных для аутентификации. **group radius** – указывает на использование серверов, определенных командой RADIUS server host. **group** *GROUP-NAME* – указывает на использование групп серверов,определенных командой AAA group

	server. **none** – обычно метод занимает в списке последнее место. Пользователь пройдет аутентификацию, если это не запрещено ему предыдущим методом аутентификации.

По умолчанию

Метод аутентификации AAA не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте эту команду для настройки списка методов аутентификации по умолчанию для аутентификации JWAC. Изначально список методов по умолчанию не настроен. Аутентификация запросов JWAC будет выполняться на основе локальной базы данных.

Пример

В этом примере показано, как установить список методов по умолчанию для аутентификации JWAC.

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

8-8 aaa authentication login

Данная команда используется для настройки списка методов по умолчанию, используемого для аутентификации с именем пользователя. Используйте форму **no** для удаления списка методов с именем пользователя по умолчанию.

aaa authentication login {default | *LIST-NAME***}** *METHOD1* **[***METHOD2***...]**
no aaa authentication login {default | *LIST-NAME***}**

Параметры

default	Указывает на настройку списка методов по умолчанию для аутентификации с именем пользователя.
LIST-NAME	Имя списка методов, отличного от списка методов по умолчанию. Длинаимени не должна превышать 32 символов.
METHOD1 [METHOD2...]	Укажите список методов, которые необходимо выполнить алгоритму аккаунтинга в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для

	указания метода. **local** – указывает на использование локальной базы данных дляаутентификации. **group radius** – указывает на использование серверов, определенных командой RADIUS server host. **group tacacs+** – указывает на использование серверов, определенных командой TACACS+ server host. **group** *GROUP-NAME* – указывает на использование групп серверов,определенных командой AAA group server. **none** – обычно метод занимает в списке последнее место. Пользователь пройдет аутентификацию, если это не запрещено ему предыдущим методом аутентификации.

По умолчанию

Метод аутентификации AAA не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для настройки списка методов аутентификации, используемого для аутентификации с именем пользователя. Можно настроить несколько списков методов. Ключевое слово по умолчанию используется для определения списка методов по умолчанию.

Если аутентификация использует список методов по умолчанию, но список методов по умолчанию отсутствует, то аутентификация будет выполняться через локальную базу данных.

Тип аутентификации по имени пользователя использует имя пользователя и пароль для входа в систему, а также назначает уровень прав доступа для пользователя на основе базы данных.

Список методов является последовательным списком, описывающим методы аутентификации, которые должны запрашиваться для того, чтобы аутентифицировать пользователя. Списки методов позволяют назначить один или несколько протоколов безопасности, которые должны использоваться для аутентификации, что обеспечивает наличие системы резервного копирования для аутентификации в случае сбоя исходного метода. Коммутационная система использует первый метод в списке для аутентификации пользователей. Если этот метод не отвечает, коммутационная система выбирает следующий метод аутентификации в списке. Этот процесс продолжается до тех пор, пока не будет установлено успешное соединение с помощью метода аутентификации из списка или пока все методы, перечисленные в списке, не будут исчерпаны.

Важно помнить, что коммутационная система пытается выполнить аутентификацию с помощью следующего метода аутентификации по списку, только когда от предыдущего метода не поступает ответа. Если происходит сбой аутентификации в любой момент данного цикла, что означает, что сервер безопасности или локальная база данных имен пользователей отвечает отказом в доступе пользователю, то процесс аутентификации останавливается и другие методы аутентификации больше не будут использоваться.

Пример

В данном примере показано, как установить список методов по умолчанию для аутентификации попыток входа в систему.

```
Switch#configure terminal
Switch(config)# aaa authentication login default group group2 local
Switch(config)#
```

8-9 aaa authentication mac-auth

Данная команда используется для настройки списка методов по умолчанию, используемого для аутентификации MAC. Используйте форму **no** для удаления списка методов по умолчанию.

aaa authentication mac-auth default *METHOD1* **[***METHOD2***...]**
no aaa authentication mac-auth default

Параметры

METHOD1 [METHOD2...]	Укажите список методов, которые необходимо выполнить алгоритму аккаунтинга в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для указания метода. **local** – указывает на использование локальной базы данных дляаутентификации. **group radius** – указывает на использование серверов, определенных командой RADIUS server host. **group** *GROUP-NAME* – указывает на использование групп серверов,определенных командой AAA group server. **none** – обычно метод занимает в списке последнее место. Пользователь пройдет аутентификацию, если это не запрещено ему предыдущим методом аутентификации.

По умолчанию

Метод аутентификации AAA не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Данная команда используется для настройки списка методов по умолчанию, используемого для аутентификации MAC. Изначально список методов по умолчанию не настроен. Аутентификация запросов MAC будет выполняться на основе локальной базы данных.

Пример

В данном примере показано, как установить список методов по умолчанию для аутентификации пользователей mac-auth.

```
Switch#configure terminal
Switch(config)# aaa authentication mac-auth default group radius
Switch(config)#
```

8-10 aaa authentication web-auth

Данная команда используется для настройки списка методов по умолчанию, используемого для аутентификации Web. Используйте форму **no** для удаления списка методов по умолчанию.

aaa authentication web-auth default *METHOD1* **[***METHOD2***...]**
no aaa authentication web-auth default

Параметры

METHOD1 [METHOD2...]	Укажите список методов, которые необходимо выполнить алгоритму аккаунтинга в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для указания метода. **local** – указывает на использование локальной базы данных для аутентификации. **group radius** – указывает на использование серверов, определенных командой RADIUS server host. **group** *GROUP-NAME* – указывает на использование групп серверов,определенных командой AAA group server. **none** – обычно метод занимает в списке последнее место. Пользователь пройдет аутентификацию, если это не запрещено ему предыдущим методом аутентификации.

По умолчанию

Метод аутентификации AAA не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Данная команда используется для настройки списка методов по умолчанию, используемого для аутентификации Web. Изначально список методов по умолчанию не настроен. Аутентификация запросов web-auth будет выполняться на основе локальной базы данных.

Пример

В данном примере показано, как установить список методов по умолчанию для аутентификации пользователей web-auth.

```
Switch#configure terminal
Switch(config)# aaa authentication web-auth default group radius
Switch(config)#
```

8-11 aaa group server radius

Данная команда используется для входа в режим настройки группы серверов RADIUS (RADIUS Group Server Configuration Mode) для связывания узлов сервера с группой. Используйте форму **no** для удаления группы серверов RADIUS.

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

Параметры

GROUP-NAME	Имя группы серверов. Длина имени не должна превышать 32 символов. Синтаксисом является обычная строка, в которой пробелы недопустимы.

По умолчанию

Группа серверов AAA не настроена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для определения группы серверов RADIUS. Созданная группа серверов используется в определении списков методов, используемых для аутентификации или аккаунтинга с помощью команд **aaa authentication** и **aaa accounting**. Также используйте данную команду для входа в режим настройки группы серверов RADIUS (RADIUS Group Server Configuration Mode). Используйте команду server для связывания узлов сервера RADIUS с группой серверов RADIUS.

Пример

В данном примере показано, как создать группу серверов RADIUS с двумя записями. Вторая запись узла выступает в качестве резервной для первой записи.

```
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)#
```

8-12 aaa group server tacacs+

Данная команда используется для входа в режим настройки группы серверов TACACS+ (TACACS+ Group Server Configuration Mode) для связывания узлов сервера с группой. Используйте форму **no** для удаления группы серверов TACACS+.

aaa group server tacacs+ *GROUP-NAME*
no aaa group server tacacs+ *GROUP-NAME*

Параметры

GROUP-NAME	Имя группы серверов. Длина имени не должна превышать 32 символов. Синтаксисом является обычная строка, в которой пробелы недопустимы.

По умолчанию

Группа серверов AAA не настроена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для входа в режим настройки группы серверов TACACS+. Используйте команду **server**, чтобы связать узлы сервера TACACS+ с группой серверов TACACS+. Определенная группа серверов может быть указана в качестве списка методов для аутентификации или аккаунтинга с помощью команд **aaa authentication** и **aaa accounting**.

Пример

В данном примере показано, как создать группу серверов TACACS+ с двумя записями.

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

8-13 aaa new-model

Данная команда используется для включения AAA для аутентификации и аккаунтинга. Используйте форму **no** для отключения функции AAA.

aaa new-model
no aaa new-model

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Пользователь должен использовать команду **aaa new-model** для включения AAA до вступления в силу аутентификации и аккаунтинга через списки методов AAA. Если функция AAA отключена, пользователь будет аутентифицирован через локальную таблицу пользовательских учетных записей,созданную командой **username**. Включение входа с паролем будет аутентифицировано через локальную таблицу, которая определяется через команду **enable password**.

Пример

В данном примере показано, как включить функцию AAA.

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

8-14 aaa server radius dynamic-author

Эта команда используется для включения коммутатора в качестве сервера AAA, чтобы облегчить взаимодействие с внешним сервером политик. Для отключения этой функции используйте форму **no** этой команды.

aaa server radius dynamic-author
no aaa server radius dynamic-author

Параметры

Нет

По умолчанию

По умолчанию эта функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Динамическая авторизация позволяет внешнему серверу политики динамически отправлять обновления на устройство. Используйте эту команду для входа в режим конфигурации локального сервера динамической авторизации и настройки команд приложения RADIUS.

Пример

В этом примере показано, как включить коммутатор в качестве сервера AAA при взаимодействии с клиентом по IP-адресу 10.12.12.12.

```
Switch#configure terminal
Switch(config)# aaa server radius dynamic-author
Switch(config-locsvr-da-radius)# client 10.12.12.12 server-key 12345
```

8-15 accounting commands

Данная команда используется для настройки списка методов, используемого для аккаунтинга команд через конкретную сессию. Используйте форму **no** для отключения аккаунтинга команд.

accounting commands *LEVEL* **{default |** *METHOD-LIST***}**
no accounting commands *LEVEL*

Параметры

LEVEL	Указывает на выполнение аккаунтинга для всех команд **configure** на указанном уровне прав доступа. Корректные записи уровней прав доступа: от 1 до 15.
default	Указывает на выполнение аккаунтинга на основе списка методов по умолчанию.
METHOD-LIST	Имя списка методов для использования.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Line Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Чтобы аккаунтинг по списку методов вступил в силу, сначала включите AAA, используя команду **aaa new-model**. Сначала создайте список методов, используя команду **aaa accounting commands**. Если список методов отсутствует, то команда не вступит в силу. Пользователь может указать разные списки методов для команд аккаунтинга (account) на разных уровнях. У уровня может быть указан только один список методов.

Пример

В данном примере показано, как включить уровень аккаунтинга команд 15 для настройки команды, вводимой через консоль, используя список методов аккаунтинга с именем «cmd-15» на консоли.

```
Switch# configure terminal
Switch(config)# aaa accounting commands 15 cmd-15 start-stop group tacacs+
Switch(config)# line console
Switch(config-line)# accounting commands 15 cmd-15
Switch(config-line)#
```

8-16 accounting exec

Данная команда используется для настройки списка методов, используемого для аккаунтинга EXEC для конкретной сессии. Используйте форму **no** для отключения опции аккаунтинга EXEC.

accounting exec {default | *METHOD-LIST***}**
no accounting exec

Параметры

default	Указывает на использование списка методов по умолчанию.
METHOD-LIST	Имя списка методов для использования.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Line Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Чтобы аккаунтинг по списку методов вступил в силу, сначала включите AAA, используя команду **aaa new-model**. Сначала создайте список методов, используя команду **aaa accounting exec**. Если списокметодов отсутствует, то команда не вступает в силу.

Пример

В данном примере показано, как настроить список методов аккаунтинга EXEC с именем “list-1”. Он использует сервер RADIUS. Если сервер безопасности не отвечает, он не выполняет аккаунтинг.

После настройки аккаунтинг EXEC применяется к консоли.

```
Switch#configure terminal
Switch(config)# aaa accounting exec list-1 start-stop group radius
Switch(config)# line console
Switch(config-line)# accounting exec list-1
Switch(config-line)#
```

8-17 clear aaa counters servers

Данная команда используется для сброса счетчиков статистики серверов AAA.

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

Параметры

all	Указывает на удаление информации счетчиков сервера, связанной со всеми узлами сервера.
radius *IP-ADDRESS*	Указывает на удаление информации счетчиков сервера, связанной с узлом RADIUS IPv4.
radius *IPV6-ADDRESS*	Указывает на удаление информации счетчиков сервера, связанной с узлом RADIUS IPv6.
radius all	Указывает на удаление информации счетчиков сервера, связанной со всеми узлами RADIUS.
tacacs *IP-ADDRESS*	Указывает на удаление информации счетчиков сервера, связанной с узлом TACACS IPv4.
tacacs all	Указывает на удаление информации счетчиков сервера, связанной со всеми узлами TACACS.
sg *NAME*	Указывает на удаление информации счетчиков сервера, связанной со всеми узлами в группе серверов.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

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

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

8-18 client

Эта команда используется для указания клиента RADIUS, от которого устройство может принимать запросы на изменение авторизации (CoA) и отключение. Для удаления клиента используйте форму **no** этой команды.

client {*IP-ADDRESS* **|** *HOST-NAME***} server-key [0 | 7]** *STRING*
no client {*HOST-NAME* **|** *IP-ADDRESS***}**

Параметры

IP-ADDRESS	Указывает на IP-адрес RADIUS-клиента.
HOST-NAME	Указывает на имя узла клиента RADIUS.
server-key	Указывает ключ RADIUS, который будет использоваться совместно Swtich и клиентом RADIUS.
0	(Опционально) Указывает пароль в виде открытого текста. Это параметр по умолчанию.
7	(Опционально) Указывает пароль в зашифрованном виде.
STRING	Указание общего ключа.

По умолчанию

Запросы CoA и разъединения отбрасываются.

Режим ввода команды

Dynamic Authorization Local Server Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте эту команду для указания клиента RADIUS. Коммутатор можно настроить так, чтобы внешний сервер политик мог динамически отправлять обновления на коммутатор. Эта функциональность обеспечивается расширением CoA RADIUS. CoA вводит одноранговую возможность RADIUS, позволяя коммутатору и внешнему серверу политики выступать в качестве клиента и сервера RADIUS.

Пример

В этом примере показано, как настроить коммутатор на прием запросов от клиента RADIUS по IP-адресу 10.0.0.1.

```
Switch# aaa server radius dynamic-author
Switch(config-locsvr-da-radius)# client 10.0.0.1 server-key 12345
```

8-19 ip http authentication aaa login-authentication

Эта команда используется для указания списка методов аутентификации AAA для аутентификации пользователей HTTP-сервера. Используйте форму **no** этой команды для возврата к использованию списка методов по умолчанию.

ip http authentication aaa login-authentication {default | *METHOD-LIST***}**
no ip http authentication aaa login-authentication

Параметры

default	Указывает на использование списка методов по умолчанию.
METHOD-LIST	Имя списка методов для использования.

По умолчанию

По умолчанию используется этот параметр **default**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Чтобы аутентификация по списку методов вступила в силу, сначала включите AAA с помощью команды **aaa new-model**. Сначала создайте список методов с помощью команды **aaa authentication login**. Если список методов не существует, команда не вступит в силу, и аутентификация будет выполняться с помощью списка методов входа по умолчанию.

Пример

В этом примере показано, как настроить сеансы HTTP на использование списка методов "WEB-METHOD" для аутентификации входа.

```
Switch# configure terminal
Switch(config)# aaa authentication login WEB-METHOD group group2 local
Switch(config)# ip http authentication aaa login-authentication WEB-METHOD
Switch(config)#
```

8-20 ip http accounting exec

Эта команда используется для указания метода учета AAA для пользователей сервера HTTP. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

ip http accounting exec {default | *METHOD-LIST***}**
no ip http accounting exec

Параметры

default	Указывает на использование списка методов по умолчанию.
METHOD-LIST	Имя списка методов для использования.

По умолчанию

По умолчанию эта опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Чтобы учет через список методов вступил в силу, сначала включите AAA с помощью команды **aaa new-model**. Сначала создайте список методов с помощью команды **aaa accounting exec**. Если список методов не существует, команда не вступит в силу.

Пример

В этом примере показано, как указать, что метод, настроенный для AAA, должен использоваться для учета пользователей HTTP-сервера. Метод учета AAA настроен как метод учета RADIUS.

```
Switch# configure terminal
Switch(config)# aaa accounting exec list-1 start-stop group radius
Switch(config)# ip http accounting exec list-1
Switch(config)#
```

8-21 ip radius source-interface

Данная команда используется для указания интерфейса, чей IP-адрес будет использоваться в качестве IP-адреса источника для отправки пакетов RADIUS. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ip radius source-interface *INTERFACE-ID*
no ip radius source-interface

Параметры

INTERFACE-ID	Указывает интерфейс, чей IP-адрес будет использоваться в качестве IP-адреса источника для отправки пакетов RADIUS.

По умолчанию

Будет использоваться IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode
Server Group Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

С помощью этой команды можно указать интерфейс, IP-адрес которого будет использоваться в качестве IP-адреса источника для отправки пакетов RADIUS. Если интерфейс источника указан и в режиме глобальной конфигурации, и в режиме конфигурации сервера группы, приоритет имеет интерфейс источника, указанный в режиме конфигурации сервера группы.

Пример

В данном примере показано, как установить VLAN100, чей IP-адрес будет использоваться в качестве IP-адреса источника для отправки пакетов RADIUS.

```
Switch#configure terminal
Switch(config)# ip radius source-interface vlan 100
Switch(config)#
```

8-22 ip tacacs source-interface

Данная команда используется для указания интерфейса, чей IP-адрес будет использоваться в качестве IP-адреса источника для отправки пакетов TACACS. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ip tacacs source-interface *INTERFACE-ID*
no ip tacacs source-interface

Параметры

INTERFACE-ID	Указывает интерфейс, чей IP-адрес будет использоваться в качестве IP-адреса источника для отправки пакетов TACACS.

По умолчанию

Будет использоваться IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode
Server Group Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Эта команда может быть использована для указания интерфейса, IP-адрес которого будет использоваться в качестве IP-адреса источника для отправки пакетов TACACS. Если интерфейс источника указан как в режиме глобальной конфигурации, так и в режиме конфигурации сервера группы, приоритет имеет интерфейс источника, указанный в режиме конфигурации сервера группы.

Пример

В данном примере показано, как установить VLAN 100, чей IP-адрес будет использоваться в качестве IP-адреса источника для отправки пакетов TACACS.

```
Switch#configure terminal
Switch(config)# ip tacacs source-interface vlan 100
Switch(config)#
```

8-23 ipv6 radius source-interface

Данная команда используется для указания интерфейса, чей IPv6-адрес будет использоваться в качестве IPv6-адреса источника для отправки пакетов RADIUS. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ipv6 radius source-interface *INTERFACE-ID*
no ipv6 radius source-interface

Параметры

INTERFACE-ID	Указывает интерфейс, чей IPv6-адрес будет использоваться в качестве IPv6- адреса источника для отправки пакетов RADIUS.

По умолчанию

Будет использоваться IPv6-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode
Server Group Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Эта команда используется для указания интерфейса, IPv6-адрес которого будет использоваться в качестве IPv6-адреса источника для отправки пакетов RADIUS. Если интерфейс источника указан и в режиме глобальной конфигурации, и в режиме конфигурации сервера группы, приоритет имеет интерфейс источника, указанный в режиме конфигурации сервера группы.

Пример

В данном примере показано, как установить VLAN 100, чей IPv6-адрес будет использоваться в качестве IP-адреса источника для отправки пакетов RADIUS.

```
Switch#configure terminal
Switch(config)# ipv6 radius source-interface vlan 100
Switch(config)#
```

8-24 ipv6 tacacs source-interface

Данная команда используется для указания интерфейса, чей IPv6-адрес будет использоваться в качестве IPv6-адреса источника для отправки пакетов TACACS. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ipv6 tacacs source-interface *INTERFACE-ID*
no ipv6 tacacs source-interface

Параметры

INTERFACE-ID	Указывает интерфейс, чей IPv6-адрес будет использоваться в качестве IPv6- адреса источника для отправки пакетов TACACS.

По умолчанию

Будет использоваться IPv6-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode
Server Group Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

С помощью этой команды можно указать интерфейс, IPv6-адрес которого будет использоваться в качестве IPv6-адреса источника для отправки пакетов TACACS. Если интерфейс источника указан и в режиме глобальной конфигурации, и в режиме конфигурации сервера группы, приоритет имеет интерфейс источника, указанный в режиме конфигурации сервера группы.

Пример

В данном примере показано, как установить VLAN 100, чей IPv6-адрес будет использоваться в качестве IP-адреса источника для отправки пакетов TACACS.

```
Switch#configure terminal
Switch(config)# ipv6 tacacs source-interface vlan 100
Switch(config)#
```

8-25 login authentication

Данная команда используется для настройки списка методов, используемого для аутентификации с именем пользователя для конкретной сессии. Используйте форму **no**, чтобы вернуться к списку методов по умолчанию.

login authentication {default | *METHOD-LIST***}**
no login authentication

Параметры

default	Указывает на аутентификацию на основе списка методов по умолчанию.
METHOD-LIST	Имя списка методов для использования.

По умолчанию

По умолчанию используется список методов по умолчанию.

Режим ввода команды

Line Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Чтобы аутентификация через список методов вступила в силу, сначала включите AAA, используя команду **aaa new-model**. Сначала создайте список методов, используя команду **aaa authenticationlogin**. Если список методов отсутствует, то команда не вступает в силу, и аутентификация будет выполняться через список методов с именем пользователя по умолчанию.

Когда включена опция **aaa new-model**, для аутентификации используется список методов поумолчанию.

Пример

В данном примере показано, как установить локальную сессию консоли для использования списка методов «CONSOLE-LINE-METHOD» для аутентификации с именем пользователя.

```
Switch#configure terminal
Switch(config)# aaa authentication login CONSOLE-LINE-METHOD group group2 local
Switch(config)# line console
Switch(config-line)# login authentication CONSOLE-LINE-METHOD
Switch(config-line)#
```

8-26 port

Эта команда используется для указания номера порта, на котором коммутатор прослушивает запросы RADIUS от настроенных клиентов RADIUS. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

port *PORT-NUMBER*
no port

Параметры

PORT-NUMBER	Укажите номер порта.

По умолчанию

По умолчанию номер порта равен 3799.

Режим ввода команды

Dynamic Authorization Local Server Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте эту команду, чтобы указать номер порта, на котором коммутатор прослушивает запросы RADIUS от настроенных клиентов RADIUS. Коммутатор можно настроить так, чтобы внешний сервер политики мог динамически отправлять обновления на коммутатор. Эта функциональность обеспечивается расширением CoA RADIUS. CoA представляет одноранговую возможность RADIUS, позволяя коммутатору и внешнему серверу политики выступать в качестве клиента и сервера RADIUS.

Пример

В этом примере показано, как указать порт номер 1650 для прослушивания запросов RADIUS.

```
Switch# aaa server radius dynamic-author
Switch(config-locsvr-da-radius)# client 10.0.0.1 server-key 12345
Switch(config-locsvr-da-radius)# port 1650
```

8-27 radius-server attribute 4

Эта команда используется для указания IP-адреса для атрибута **radius-server attribute 4**. Используйте форму **no** этой команды для удаления IP-адреса.

radius-server attribute 4 *IP-ADDRESS*
no radius-server attribute 4 *IP-ADDRESS*

Параметры

IP-ADDRESS	Указывает IP-адрес для radius-server attribute 4.

По умолчанию

По умолчанию IP-адрес -это IP-адрес интерфейса, соединяющего NAS с сервером RADIUS.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Обычно, когда настроена команда **ip radius source-interface**, указанный IP-адрес используется как IP-адрес в IP-заголовках пакетов RADIUS и как адрес атрибута 4 RADIUS внутри пакетов RADIUS.

Однако, когда настроена команда **radius-server attribute 4**, указанный IP-адрес используется в качестве адреса RADIUS attribute 4 внутри пакетов RADIUS. IP-адрес в IP-заголовках пакетов RADIUS не изменяется.

Пример

В этом примере показано, как настроить адрес атрибута 4 RADIUS как 10.0.0.21.

```
Switch# configure terminal
Switch(config)#radius-server attribute 4 10.0.0.21
Switch(config)#
```

8-28 radius-server attribute 55 include-in-acct-req

Эта команда используется для включения отправки атрибута RADIUS 55 (Event-Timestamp) в пакетах учета. Для отключения этой функции используйте форму **no** этой команды.

radius-server attribute 55 include-in-acct-req
no radius-server attribute 55 include-in-acct-req

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте эту команду для включения или отключения отправки атрибута RADIUS 55 в пакетах учета. Атрибут Event-Timestamp записывает время, когда событие произошло на NAS. Временная метка отправляется в атрибуте 55 в секундах с 1 января 1970 года 00:00 UTC.

Пример

В этом примере показано, как включить отправку атрибута RADIUS 55.

```
Switch#configure terminal
Switch(config)# radius-server attribute 55 include-in-acct-req
Switch(config)#
```

8-29 radius-server deadtime

Данная команда используется для указания времени по умолчанию, по истечении которого сервер, который не может ответить, будет пропущен. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Параметры

MINUTES	Время простоя. Корректный диапазон: от 0 до 1440 (24 часа). Если установлено значение 0, сервер, который не может ответить, не будет помечен как недействующий.

По умолчанию

По умолчанию данным значением является 0.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Данная команда может использоваться для улучшения времени процесса аутентификации с помощью установки времени простоя (dead time) для пропуска записей узлов сервера, который не может ответить.

Когда система выполняет аутентификацию с помощью сервера аутентификации, она пробует использовать один сервер за раз. Если сервер не отвечает, система будет пробовать следующий сервер. Когда система обнаруживает, что сервер не отвечает, она пометит сервер как недействующий, запустит таймер времени простоя и пропустит их при аутентификации последующих запросов до истечения времени простоя.

Пример

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

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

8-30 radius-server host

Данная команда используется для создания узла сервера RADIUS. Используйте форму **no** для удаления узла сервера.

radius-server host {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [auth-port** *PORT***] [acct-port** *PORT***][timeout** *SECONDS***] [retransmit** *COUNT***] key [0 | 7]** *KEY-STRING*
no radius-server host {*IP-ADDRESS* **|** *IPV6-ADDRESS***}**

Параметры

IP-ADDRESS	IP-адрес сервера RADIUS.
IPV6-ADDRESS	IPv6-адрес сервера RADIUS.
auth-port *PORT-NUMBER*	(Опционально) Номер UDP-порта назначения для отправки пакетов аутентификации. Диапазон: от 0 до 65535. Укажите ноль в качестве значения номера порта, если узел сервера не предназначен для аутентификации. Значение по умолчанию - 1812.
acct-port *PORT-NUMBER*	(Опционально) Номер UDP-порта назначения для отправки пакетов аккаунтинга. Диапазон: от 0 до 65535. Укажите ноль в качестве значения номера порта, если узел сервера не предназначен для аккаунтинга. Значение по умолчанию: 1813.
timeout *SECONDS*	Значение тайм-аута сервера. Диапазон: от 1 до 255 секунд. Если значение не указано, то значением по умолчанию является 5 секунд.
retransmit *COUNT*	(Опционально) Количество повторных передач запросов на сервер, когда ответ не получен. Значение: от 0 до 20. Используйте 0 для отключения повторной передачи. Если значение не указано, то значением по умолчанию является 2.
0	(Опционально) Пароль в форме обычного незашифрованного текста. Это является опцией по умолчанию.
7	(Опционально) Пароль в зашифрованной форме.
key *KEY-STRING*	Ключ, используемый для связи с сервером. Длина ключа может составлять от 1 до 32 символов незашифрованного текста.

По умолчанию

По умолчанию сервер не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

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

```
Switch#configure terminal
Switch(config)# radius-server host 172.19.10.100 auth-port 1500 acct-port 1501 timeout 8
retransmit 3 key ABCDE
Switch(config)# radius-server host 172.19.10.101 auth-port 1600 acct-port 1601 timeout 3
retransmit 1 key ABCDE
Switch(config)#
```

8-31 server (RADIUS)

Данная команда используется для связывания узла сервера RADIUS (RADIUS server host) с группой серверов RADIUS (RADIUS server group). Используйте форму **no** для удаления узла сервера из группы серверов.

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

Параметры

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

По умолчанию

По умолчанию сервер не настроен.

Режим ввода команды

RADIUS Group Server Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для входа в режим настройки группы серверов RADIUS (RADIUS GroupServer Configuration Mode). Используйте команду **server** для связывания узлов сервера RADIUS с группой серверов RADIUS. Определенная группа серверов может быть указана в качестве списка методов для аутентификации или аккаунтинга через команды **aaa authentication** и **aaa accounting**. Используйте команду **radius-server host** для создания записи узла сервера. Запись узла идентифицируется IP-адресом.

Пример

В данном примере показано, как создать два узла сервера RADIUS с разными IP-адресами. Группа серверов затем создается с двумя узлами 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)#
```

8-32 server (TACACS+)

Данная команда используется для связывания сервера TACACS+ с группой серверов. Используйте форму **no** для удаления сервера из группы серверов.

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

Параметры

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

По умолчанию

По умолчанию сервер не настроен.

Режим ввода команды

TACACS+ Group Server Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте команду **aaa group server tacacs+** для входа в режим настройки группы серверов TACACS+ (TACACS+ group server configuration mode). Используйте команду **server** для связывания узлов сервера TACACS+ с группой серверов TACACS+. Определенная группа серверов может быть указана в качестве списка методов для аутентификации или аккаунтинга через команды **aaa authentication** и **aaa accounting**. Используйте команду **tacacs-server host** для создания записи узласервера. Запись узла идентифицируется IP-адресом.

Пример

В данном примере показано, как создать два узла сервера TACACS+ с разными IP-адресами. Группа серверов затем создается с двумя узлами серверов.

```
Switch#configure terminal
Switch(config)# tacacs-server host 172.19.10.100 port 1500 timeout 8 key ABCDE
Switch(config)# tacacs-server host 172.19.122.3 port 1600 timeout 3 key ABCDE
Switch(config)#aaa group server tacacs+ group2
Switch(config-sg-tacacs+)# server 172.19.10.100
Switch(config-sg-tacacs+)# server 172.19.122.3
Switch(config-sg-tacacs+)#
```

8-33 show aaa

Данная команда используется для отображения глобального состояния AAA.

show aaa

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду для отображения глобального состояния AAA.

Пример

В данном примере показано, как отобразить глобальное состояние AAA.

```
Switch# show aaa

AAA is enabled.

Switch#
```

8-34 tacacs-server host

Данная команда используется для создания узла сервера TACACS+. Используйте форму **no** для удаления узла сервера.

tacacs-server host {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [port** *PORT***] [timeout** *SECONDS***] key [0 |7]** *KEY-STRING*

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

Параметры

IP-ADDRESS	IPv4-адрес сервера аутентификации.
IPV6-ADDRESS	IPv6-адрес сервера аутентификации.
port *PORT-NUMBER*	(Опционально) Номер UDP-порта назначения для отправки пакетов с запросами. Номер порта по умолчанию – 49. Диапазон: от 1 до 65535.
timeout ***SECONDS***	Значение тайм-аута сервера. Диапазон: от 1 до 255 секунд. Значением по умолчанию является 5 секунд.
0	(Опционально) Пароль в форме обычного незашифрованного текста. Это является опцией по умолчанию.
7	(Опционально) Пароль в зашифрованной форме.
key *KEY-STRING*	Ключ, используемый для связи с сервером. Длина ключа может составлять от 1 до 254 символов незашифрованного текста.

По умолчанию

По умолчанию узел сервера TACACS+ не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте команду **tacacs-server host** для создания узлов сервера TACACS+ перед тем, как они могут быть связаны с группой серверов TACACS+ с помощью команды **server**.

Пример

В данном примере показано, как создать два узла сервера TACACS+ с разными IP-адресами.

```
Switch#configure terminal
Switch(config)# tacacs-server host 172.19.10.100 port 1500 timeout 8 key ABCDE
Switch(config)# tacacs-server host 172.19.122.3 port 1600 timeout 3 key ABCDE
Switch(config)#
```

8-35 show radius statistics

Данная команда используется для отображения статистики RADIUS для пакетов аккаунтинга и аутентификации.

show radius statistics

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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: 172.19.192.80: Auth-Port 1645, Acct-Port 1646
State is UP
                              Auth.   Acct.
Round Trip Time:              10      10
Access Requests:               4      NA
Access Accepts:                0      NA
Access Rejects:                4      NA
Access Challenges:             0      NA
Acct Request:                 NA       3
Acct Response:                NA       3
Retransmissions:               0       0
Malformed Responses:           0       0
Bad Authenticators:            0       0
 Pending Requests:             0       0
 Timeouts:                     0       0
 Unknown Types:                0       0
 Packets Dropped:              0       0
```

Отображаемые параметры

Auth.	Статистика для пакетов аутентификации
Acct.	Статистика для пакетов аккаунтинга.
Round Trip Time	Интервал времени (в сотых долях секунды) между самым 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.
Acct Request	Количество отправленных пакетов RADIUS Accounting-Request. Не включает повторные передачи.
Acct Response	Количество пакетов RADIUS, полученных на accounting-порту от данного сервера.
Retransmissions	Количество пакетов RADIUS Request, повторно переданных данному серверу RADIUS. Повторные передачи включают записи, где идентификатор и Acct-Delay были обновлены, так же как и те, в которых они остаются одинаковыми.
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 включаются в ошибочные ответы.
Bad Authenticators	Количество пакетов RADIUS Response, содержащих некорректные аутентификаторы или атрибуты Signature, полученных от данного сервера.
Pending Requests	Количество пакетов RADIUS Request, предназначенных для данного сервера, время которых еще не истекло, или не получивших ответ. Эта переменная увеличивается, когда запрос отправляется, и уменьшается из-за приема ответа, тайм-аута или повторной передачи.
Timeouts	Количество тайм-аутов для данного сервера. После тайм-аута клиент может повторить попытку с тем же сервером, отправить другому серверу или отказаться. Повторная попытка с тем же сервером считается как повторная передача, а также как тайм-аут. Отправка другому серверу считается как запрос, а также как тайм-аут.
Unknown Types	Количество пакетов RADIUS неизвестного типа, полученных от данного сервера.
Packets Dropped	Количество пакетов RADIUS неизвестного типа, полученных от данного сервера и отброшенных по какой-либо причине.

8-36 show tacacs statistics

Данная команда используется для отображения условий взаимодействия с каждым сервером TACACS+.

show tacacs statistics

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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 tacacs statistics
TACACS+ Server: 172.19.192.80/49, State is UP
Socket Opens: 0
Socket Closes: 0
Total Packets Sent: 0
Total Packets Recv: 0
Reference Count: 0
```

Отображаемые параметры

TACACS+ Server	IP-адрес сервера TACACS+.
Socket Opens	Количество успешных подключений TCP socket к серверу TACACS
Socket Closes	Количество успешно закрытых попыток TCP socket.
Total Packets Sent	Количество пакетов, отправленных серверу TACACS+
Total Packets Recv	Количество пакетов, полученных от сервера TACACS+.
Reference Count	Количество запросов аутентификации от сервера TACACS+.

9. Базовые команды настройки IPv4

9-1 arp

Данная команда используется для добавления статической записи в кэш ARP (Address Resolution Protocol). Используйте форму **no**, чтобы удалить статическую запись из кэша ARP (Address Resolution Protocol).

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

Уровень команды по умолчанию

Уровень 12

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 примере показан процесс добавления статической ARP-записи для традиционного 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. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

arp timeout *MINUTES*
no arp timeout

Параметры

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

По умолчанию

По умолчанию установлено 240 минут.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки времени старения ARP-записей в таблице ARP.Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

Пример

В данном примере показано, как задать тайм-аут продолжительностью 60 минут, чтобы записи устаревали быстрее, чем это позволяют настройки по умолчанию.

```
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-ID	Укажите идентификатор интерфейса (Interface ID).
IP-ADDRESS	Укажите IP-адрес динамической ARP-записи, которую необходимо удалить.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

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 первичного или вторичного адреса IPv4 или автоматического получения IP-адреса от DHCP-сервера. Используйте форму **no**, чтобы удалить настройки IP-адреса или отключить DHCP на интерфейсе.

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

Параметры

IP-ADDRESS	Укажите IP-адрес.
SUBNET-MASK	Укажите маску подсети для соответствующего IP-адреса.
secondary	(Опционально) Укажите, если настроенный адрес является вторичным IP-адресом. Если данное ключевое слово не указано, настроенный адрес будет являться первичным IP-адресом.
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

Уровень команды по умолчанию

Уровень 12

Использование команды

IPv4-адрес интерфейса может быть назначен вручную пользователем или динамически назначен сервером DHCP. При ручном назначении пользователь может назначить несколько сетей в VLAN, каждая из которых имеет IP-адрес. Среди этих нескольких IP-адресов один должен быть основным, а остальные - вторичными.

Первичный адрес будет использоваться в качестве IP-адреса источника для сообщений SNMP-ловушек или сообщений SYSLOG, которые отправляются с интерфейса.

Пример

В данном примере показано, как настроить 10.108.1.27 в качестве основного адреса, а 192.31.7.17 и 192.31.8.17 в качестве второстепенных адресов для VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan 100
Switch(config-if)# ip address 10.108.1.27 255.255.255.0
Switch(config-if)# ip address 192.31.7.17 255.255.255.0 secondary
Switch(config-if)# ip address 192.31.8.17 255.255.255.0 secondary
Switch(config-if)#
```

9-5 ip proxy-arp

Данная команда используется для включения опции proxy ARP для интерфейса. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ip proxy-arp
no ip proxy-arp

Параметры

Нет

По умолчанию

Данная опция по умолчанию отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для настройки на интерфейсе опции proxy ARP. При включении proxy ARP система будет отвечать на запросы ARP для IP-адресов локальных подсетей. Механизм proxy ARP может использоваться в сети, где для узлов не настроен шлюз по умолчанию.

Пример

В данном примере показано, как включить proxy ARP для интерфейса VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan 100
Switch(config-if)# ip proxy-arp
Switch(config-if)#
```

9-6 ip local-proxy-arp

Данная команда используется для включения на интерфейсе опции local proxy ARP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ip local-proxy-arp
no ip local-proxy-arp

Параметры

Нет

По умолчанию

Данная опция по умолчанию отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для включения опции local proxy ARP на интерфейсе. Команда используется в основной VLAN, относящейся к домену изолированной сети VLAN, для включения маршрутизации пакетов между второстепенными сетями VLAN или изолированными портами в пределах домена. Команда сработает только после включения опции i**p arp proxy**.

Пример

В данном примере показано, как включить local proxy ARP на интерфейсе VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan 100
Switch(config-if)# ip local-proxy-arp
Switch(config-if)#
```

9-7 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 определенной сетью.
HARDWARE-ADDRESS	(Опционально) Укажите, если необходимо отобразить ARP-записи, чей аппаратный адрес равен данному MAC-адресу.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда позволяет 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#
```

9-8 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 (ID).

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения заданного времени старения ARP-записей.

Пример

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

```
Switch#show arp timeout

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

Switch#
```

9-9 show ip interface

Данная команда используется для отображения информации по IP-интерфейсу.

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

Параметры

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

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Если параметр не указан, будет отображаться информация для всех интерфейсов.

Пример

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

```
Switch#show ip interface brief

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

Total Entries: 1

Switch#
```

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

```
Switch#show ip interface vlan 1

Interface vlan1 is enabled, Link status is up
  IP Address is 10.90.90.90/8 (Manual)
  ARP timeout is 240 minutes.
  Helper Address is not set
  Proxy ARP is disabled
  IP Local Proxy ARP is disabled
  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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется 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 vlan 1
Switch#
```

10-2 ipv6 address

Данная команда используется для ручной настройки IPv6-адреса на интерфейсе. Используйте форму **no**, чтобы удалить заданный вручную IPv6-адрес.

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

Уровень команды по умолчанию

Уровень 12

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 бит, исключая часть основного префикса в оставшейся части бит.

Интерфейсу можно назначить несколько IPv6-адресов, используя для этого различные механизмы, включая ручную настройку, настройку адресов без сохранения состояния (Stateless address configuration) и настройку адресов с сохранением состояния (Stateful address configuration).

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 показана настройка IPv6-адреса.

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

В данном примере 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

Эта команда используется для настройки IPv6-адреса на интерфейсе с помощью идентификатора интерфейса EUI-64. Используйте форму **no** этой команды для удаления IPv6-адреса, сформированного с помощью идентификатора интерфейса EUI-64.

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

Параметры

IPV6-ADDRESS	Указывает часть префикса IPv6 для настроенного IPv6-адреса.
PREFIX-LENGTH	Указывает длину префикса. Префикс адреса IPv6 также является локальной подсетью интерфейса. Длина префикса должна быть меньше 64.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если команда настроена на туннель IPv6 ISTAP, последние 32 бита идентификатора интерфейса строятся с использованием IPv4-адреса источника туннеля.

Пример

В этом примере показано, как добавить адресную базу IPv6.

```
Switch# configure terminal
Switch(config)# interface vlan1
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. Для отключения использования DHCPv6 на получение IPv6-адреса воспользуйтесь формой **no**.

ipv6 address dhcp [rapid-commit]
no ipv6 address dhcp

Параметры

rapid-commit	Укажите для получения адреса от сервера благодаря обмену двумя сообщениями. Опция rapid-commit будет указана в сообщении Solicit для запроса на подтверждение двумя сообщениями.

По умолчанию

По умолчанию эта опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки интерфейса на использование DHCPv6- сервера для получения IPv6-адреса. При использовании команды **no ipv6 address dhcp** предыдущий IP-адрес, полученный от DHCPv6-сервера, будет удален. Если в команде указывается ключевое слово **rapid-commit**, то в сообщение Solicit добавляется запрос на подтверждение двумя сообщениями для получения адреса.

Пример

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

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

10-5 ipv6 enable

Данная команда используется для включения обработки IPv6 на интерфейсах, у которых нет явно настроенного IPv6-адреса. Используйте форму **no**, чтобы отключить обработку IPv6 на интерфейсах, у которых нет явно настроенного IPv6-адреса.

ipv6 enable
no ipv6 enable

Параметры

Нет

По умолчанию

Данная опция по умолчанию отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

10-6 ipv6 hop-limit

Данная команда используется для настройки параметра Hop Limit (предельное число шагов) для IPv6 на коммутаторе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Параметры

VALUE	Укажите диапазон значений для параметра IPv6 Hop Limit. Если задан 0, для отправки пакета используются настройки по умолчанию. Допустимые значения: от 0 до 255.

По умолчанию

Значение по умолчанию – 64.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для настройки параметра Hop Limit, который будет анонсироваться в сообщениях RA. Пакет IPv6, сгенерированный в системе, также будет использовать это значение в качестве начального значения параметра Hop Limit.

Пример

В этом примере показано, как настроить значение ограничения IPv6 hop limit на 255.

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

10-7 ipv6 nd managed-config-flag

Данная команда используется для включения флага Managed Configuration (M) в анонсируемых сообщениях RA. Для выключения флага используйте форму **no**.

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

Уровень команды по умолчанию

Уровень 12

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)#
```

10-8 ipv6 nd other-config-flag

Данная команда используется для включения флага Other Configuration (O) в анонсируемых сообщениях RA. Для выключения флага используйте форму **no**.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Когда эта функция включена, маршрутизатор будет инструктировать подключенные узлы использовать протокол конфигурации с состоянием для получения информации об автоконфигурации, отличной от адреса IPv6.

Пример

В этом примере показано, как включить флаг IPv6 other configure в RA, рекламируемых в VLAN 1.

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

10-9 ipv6 nd prefix

Данная команда используется для настройки IPv6-префикса, который будет анонсироваться в сообщениях RA. Для удаления префикса используйте форму **no**.

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	Введите здесь префикс IPv6, который будет создан или рекламироваться в RA на интерфейсе.
PREFIX-LENGTH	Введите здесь длину префикса IPv6, который будет создан или рекламироваться в RA на интерфейсе.
VALID-LIFETIME	(Опционально) Введите здесь действительное значение времени жизни. Диапазон составляет от 0 до 4294967295 секунд.
PREFERRED-LIFETIME	(Опционально) Введите здесь предпочтительное значение времени жизни. Диапазон составляет от 0 до 4294967295 секунд.
off-link	(Опционально) Указывает на отключение флага включения.
no-autoconfig	(Опционально) Указывает на отключение флага автоконфигурации.

По умолчанию

По умолчанию допустимое значение времени жизни составляет 2592000 секунд (30 дней).
Предпочтительное значение времени жизни по умолчанию - 604800 секунд (7 дней).
По умолчанию флаг отключения и флаг автоконфигурации включен.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Для префикса допустимое время жизни должно быть больше, чем предпочтительное время жизни. Они имеют смысл, если у префикса включен бит A. Полученный узел выполнит конфигурацию адреса без статического состояния на основе префикса. Если время жизни префикса превысило предпочтительное время жизни, то IPv6-адрес, сконфигурированный на основе этого префикса, перейдет в состояние deprecated. Если время жизни префикса превысило допустимое время жизни, то IPv6-адрес, сконфигурированный на основе этого префикса, будет удален.
Если IPv6-адрес сконфигурирован на интерфейсе вручную, соответствующий префикс будет автоматически рекламироваться. Рекламируемый префикс можно изменить, но нельзя удалить с помощью этой команды. Если IPv6-адрес будет удален позже, реклама соответствующего префикса также будет остановлена.

Пример

В этом 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)#
```

10-10 ipv6 nd ra interval

Данная команда используется для настройки временного интервала между сообщениями RA для IPv6-интерфейса.

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). Допустимые значения: от 4 до 1800 секунд.
MIN-SECS	(Опционально) Укажите минимальный временной интервал для повторной передачи сообщения RA (в секундах). Допустимые значения: от 3 до 1350 секунд

По умолчанию

Максимальный временной интервал по умолчанию – 200 секунд.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Следующие правила применяются к минимальному значению интервала RA, если минимальное значение не настроено:

- Если максимальное значение интервала RA равно или больше 9 секунд, то минимальное значение будет составлять 33% от максимального значения.
- Если максимальное значение интервала RA меньше 9 секунд, то минимальное значение будет равно максимальному значению.

Пример

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

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

10-11 ipv6 nd ra lifetime

Данная команда используется для настройки значения времени жизни (Lifetime) в анонсируемых сообщениях RA. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Параметры

SECONDS	Укажите время жизни для использования маршрутизатора в качестве маршрутизатора по умолчанию (в секундах). Допустимые значения: от 0 до 9000.

По умолчанию

Значение по умолчанию – 1800 секунд.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

В этом примере показано, как настроить значение времени жизни, рекламируемое в RA, на 9000 секунд.

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

10-12 ipv6 nd suppress-ra

Данная команда используется для отключения отправки сообщений RA на интерфейсе. Для включения отправки сообщений RA используйте форму **no**.

ipv6 nd suppress-ra
no ipv6 nd suppress-ra

Параметры

Нет

По умолчанию

По умолчанию эта функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду, чтобы отключить отправку RA-сообщений на интерфейсе. Используйте команду no для повторно включить отправку RA-сообщений на туннельном интерфейсе ISATAP.

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)#
```

10-13 ipv6 nd reachable-time

Данная команда используется для настройки параметра Reachable Time (время доступности) в таблице ND-протокола. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Параметры

MILLI-SECONDS	Введите здесь время досягаемости, используемое в протоколе ND. Диапазон от 0 до 3600000 миллисекунд с кратностью 1000 миллисекунд.

По умолчанию

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

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 в VLAN 1 значение Reachable Time продолжительностью 3600 секунд.

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

10-14 ipv6 nd ns-interval

Данная команда используется для настройки временного интервала между повторными отправками сообщений NS. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Параметры

MILLI-SECONDS	Укажите временной интервал между отправками запросов NS (в миллисекундах). Допустимые значения: 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

Уровень команды по умолчанию

Уровень 12

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)#
```

10-15 ipv6 neighbor

Данная команда используется для создания статической записи в таблице IPv6 neighbor. Используйте форму **no**, чтобы удалить статическую запись из таблицы.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для создания статической записи кэша соседей IPv6 на интерфейсе. Статическая запись будет находиться либо в состоянии REACHABLE, если интерфейс UP, либо в состоянии INCOMPLETE, если интерфейс down. Процесс обнаружения достижимости не будет применяться к статическим записям.

Команда **clear ipv6 neighbors** очистит записи кэша динамических соседей. Используйте команду **no ipv6 neighbor** для удаления записи статического соседа.

Пример

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

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

10-16 show ipv6 interface

Данная команда используется для просмотра информации по IPv6-интерфейсу.

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

Параметры

INTERFACE-ID	(Опционально) Укажите интерфейс для получения информации по нему.
brief	(Опционально) Укажите, чтобы получить краткую информацию.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду для отображения конфигураций, связанных с интерфейсом IPv6.

Пример

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

```
Switch# show ipv6 interface vlan 2

vlan 2 is up, Link status is down
  IPv6 is enabled,
  link-local address:
      FE80::201:1FF:FE02:305
  Global unicast address:
      200::2/64 (DHCPv6 PD)
  IPv6 MTU is 1500 bytes
  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

Switch#
```

В данном примере 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#
```

10-17 show ipv6 neighbors

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

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

Параметры

INTERFACE-ID	Укажите интерфейс для отображения информации о записях в таблице IPv6 neighbor cache.
IPV6-ADDRESS	Укажите IPv6-адрес, чтобы получить для него информацию о записях в таблице IPv6 neighbor cache.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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

Тип записи	**D** – динамическая изученная запись. **S** – статическая neighbor-запись.
Состояние записи	**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 моментаполучения последнего подтверждения прошло больше заданноготаймером Reachable Time времени (в миллисекундах). **PROBE** – состояние записи, при котором устройство отправляет сообщение Neighbor Solicitation, чтобы подтвердить достижимость.

11. Команды BPDU Protection

11-1 spanning-tree bpdu-protection (global)

Данная команда используется для общего включения функции BPDU Protection. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

spanning-tree bpdu-protection
no spanning-tree bpdu-protection

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду, чтобы включить защиту от атак BPDU глобально.

Пример

В этом примере показано, как включить функцию защиты от атак BPDU глобально.

```
Switch# configure terminal
Switch(config)# spanning-tree bpdu-protection
Switch(config)#
```

11-2 spanning-tree bpdu-protection (Interface)

Данная команда используется для включения функции BPDU Protection на порту. Используйте форму **no**, чтобы отключить функцию BPDU Protection на порту.

spanning-tree bpdu-protection {drop | block | shutdown}
no spanning-tree bpdu-protection

Параметры

drop	Укажите, чтобы отбросить все принимаемые BPDU-пакеты при обнаружении атаки.

block	Укажите, чтобы отбросить все пакеты (включая BPDU и обычные пакеты) при обнаружении атаки.
shutdown	Укажите, чтобы отключить интерфейс при обнаружении атаки.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

В сети клиенты не хотят, чтобы все порты устройства могли принимать пакеты STP, поскольку порты могут принимать пакеты STP BPDU, которые приводят к нерациональному использованию системных ресурсов.

Функция защиты от атак BPDU может предотвратить получение портами пакетов BPDU. Порты с включенной функцией защиты BPDU переходят в состояние защиты и при получении пакета STP BPDU реагируют одним из действий: **сброс**, **блокировка** или **выключение**.

- drop - отбросить только пакеты принятых STP BPDU, и порт переходит в нормальное состояние.
- block - отбросить пакеты полученных всех BPDU и всех данных, и порт переходит в нормальное состояние.
- shutdown - выключить порт, при этом порт переходит в состояние err-disabled.

Пример

В данном примере показано, как включить функцию BPDU Protection в режиме block на Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# spanning-tree bpdu-protection block
Switch(config-if)#
```

11-3 show spanning-tree bpdu-protection

Данная команда используется для отображения информации о BPDU Protection.

show spanning-tree bpdu-protection [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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения информации о BPDU Protection. Если не указан ID ни одного из интерфейсов, будет отображена информация обо всех интерфейсах.

Пример

В данном примере отображена информация о BPDU Protection и статусах интерфейсов.

```
Switch#show spanning-tree bpdu-protection

 Global State:      Enabled

Interface          State        Mode         Status
---------------    --------     --------     ------------
eth1/0/1           Enabled      Shutdown     Under Attack
eth1/0/2           Enabled      Drop         Normal
eth1/0/3           Disabled     Block        -
eth1/0/4           Disabled     Shutdown     Normal
eth1/0/5           Disabled     Shutdown     Normal
eth1/0/6           Disabled     Shutdown     Normal
eth1/0/7           Disabled     Shutdown     Normal
eth1/0/8           Disabled     Shutdown     Normal
eth1/0/9           Disabled     Shutdown     Normal
eth1/0/10          Disabled     Shutdown     Normal
eth1/0/11          Disabled     Shutdown     Normal
eth1/0/12          Disabled     Shutdown     Normal
eth1/0/13          Disabled     Shutdown     Normal
eth1/0/14          Disabled     Shutdown     Normal
eth1/0/15          Disabled     Shutdown     Normal
eth1/0/16          Disabled     Shutdown     Normal
eth1/0/17          Disabled     Shutdown     Normal
eth1/0/18          Disabled     Shutdown     Normal
eth1/0/19          Disabled     Shutdown     Normal
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

В данном примере отображена информация статуса BPDU Protection для Ethernet 1/0/1.

```
Switch#show spanning-tree bpdu-protection interface ethernet 1/0/1

Interface          State        Mode         Status
---------------    --------     --------     ------------
eth1/0/1           Enabled      Shutdown     Under Attack

Switch#
```

Отображаемые параметры

Interface	На интерфейсе включена функция BPDU Protection.
State	Отображает состояние конфигурации интерфейса.
Mode	Отображает режим работы интерфейса.
Status	Указывает, находится ли интерфейс в состоянии защиты.

11-4 snmp-server enable traps stp-bpdu-protection

Данная команда используется для запуска отправки SNMP-уведомлений (notification) для BPDU Protection. Используйте форму **no**, чтобы отключить отправку SNMP-уведомлений (notification) для BPDU Protection.

snmp-server enable traps stp-bpdu-protection
no snmp-server enable traps stp-bpdu-protection

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для включения или отключения отправки SNMP-уведомлений для защиты BPDU.

Пример

В данном примере показано, как включить отправку SNMP-уведомлений (notification) для BPDU Protection.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps stp-bpdu-protection
Switch(config)#
```

12. Команды Cable Diagnostics

12-1 test cable-diagnostics

Данная команда используется для запуска диагностики кабеля, предполагающей анализ состояния и длины медных кабелей.

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

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для настройки физических портов. Диагностика кабеля позволяет выявить проблемы с подключением на медных портах. Для запуска диагностики используйте команду **test cable-diagnostics**. Медный порт может находиться в одном из следующих состояний:

- **Open:** кабель не подключен к ответному устройству.
- **Short:** замыкание в одной паре кабеля.
- **Open or Short:** кабель не подключен к ответному устройству или обнаружено замыкание водной паре кабеля, но PHY не удается распознать тип неисправности.
- **Crosstalk:** замыкание между разными парами кабеля.
- **Shutdown:** удаленный партнер отключен.
- **Unknown:** неизвестное состояние диагностики кабеля.
- **OK:** неисправностей витой пары/кабеля не выявлено.
- **No cable:** на порту отсутствует подключение к удаленному партнеру.

Пример

В данном примере показано, как запустить диагностику кабеля для анализа статуса и длины медных кабелей.

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

12-2 show cable-diagnostics

Данная команда используется для просмотра результатов диагностики кабеля.

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

Параметры

interface *INTERFACE-ID*	(Опционально) Укажите ID интерфейса. Допустимым интерфейсом является физический порт.
,	(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

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения результатов диагностики кабеля.

Пример

Просмотр результатов диагностики кабеля.

```
Switch#show cable-diagnostics

Port      Type       Link Status   Test Result                Cable Length (M)
--------- ---------- ------------- ------------------------- -----------------
eth1/0/1  1000BASE-T Link Down     Shutdown                  2
eth1/0/2  1000BASE-T Link Down     -                         -
eth1/0/3  1000BASE-T Link Down     -                         -
eth1/0/4  1000BASE-T Link Down     -                         -
eth1/0/5  1000BASE-T Link Down     -                         -
eth1/0/6  1000BASE-T Link Down     -                         -
eth1/0/7  1000BASE-T Link Down     -                         -
eth1/0/8  1000BASE-T Link Down     -                         -
eth1/0/9  1000BASE-T Link Down     -                         -
eth1/0/10 1000BASE-T Link Down     -                         -
eth1/0/11 1000BASE-T Link Down     -                         -
eth1/0/12 1000BASE-T Link Down     -                         -
eth1/0/13 1000BASE-T Link Down     -                         -
eth1/0/14 1000BASE-T Link Down     -                         -
eth1/0/15 1000BASE-T Link Down     -                         -
eth1/0/16 1000BASE-T Link Down     -                         -
eth1/0/17 1000BASE-T Link Down     -                         -
eth1/0/18 1000BASE-T Link Down     -                         -
eth1/0/19 1000BASE-T Link Down     -                         -
eth1/0/20 1000BASE-T Link Down     -                         -
eth1/0/21 1000BASE-T Link Down     -                         -
eth1/0/22 1000BASE-T Link Down     -                         -
eth1/0/23 1000BASE-T Link Down     -                         -
eth1/0/24 1000BASE-T Link Down     -                         -

Switch#
```

12-3 clear cable-diagnostics

Данная команда используется для очистки результатов диагностики кабеля.

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

Параметры

all	Используется для очистки результатов диагностики кабеля для всех интерфейсов.
interface *INTERFACE-ID*	Укажите ID интерфейса. Допустимым интерфейсом является физический порт.
,	(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

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для очистки результатов диагностики кабеля. При проведении диагностики на интерфейсе будет отображена ошибка.

Пример

В данном примере показано, как очистить результаты диагностики кабеля.

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

13. Команды логирования выполненных команд

13-1 command logging enable

Данная команда используется для включения функции логирования выполненных команд. При использовании формы **no** команда отключит функцию логирования.

command logging enable
no command logging enable

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команды логирования используются для записи списка команд, успешно выполненных через интерфейс командной строки. В журнале ведется запись введенных команд и информации об учетной записи пользователя, в которой была введена команда. Команды, не изменяющие конфигурацию или работу коммутатора (например, **show**), не записываются. Информация о сохранении и просмотре системного журнала описана в характеристиках sys-log.

Примечание: если коммутатор находится в режиме BAT (процедура загрузки, загрузка конфигурационного файла и т.д.), никакая из команд конфигурации не логируется (не будет записана в журнал).

Пример

В данном примере показан процесс включения функции логирования.

```
Switch# configure terminal
Switch(config)# command logging enable
Switch(config)#
```

14. Команды Debug

14-1 debug reboot on-error

Данная команда используется для включения режима перезапуска коммутатора при возникновении критических ошибок. Используйте форму **no**, чтобы отключить режим перезапуска при возникновении критических ошибок.

debug reboot on-error
no debug reboot on-error

Параметры

Нет

По умолчанию

По умолчанию данный режим включен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

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)#
```

14-2 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.
LOCATION	Укажите адрес IPv4 или IPv6 TFTP-сервера.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для копирования информации по отладке в указанный файл.

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#
```

14-3 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

Уровень команды по умолчанию

Уровень 15

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#
```

14-4 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

Уровень команды по умолчанию

Уровень 15

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#
```

14-5 debug show tech-support

Эта команда используется для отображения информации, необходимой персоналу технической поддержки.

debug show tech-support [unit *UNIT-ID***]**

Параметры

unit *UNIT-ID*	(Опционально) Указывает идентификатор устройства в стеке. Если не указан, отображаются все устройства.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте эту команду для отображения информации технической поддержки. Информация технической поддержки используется для сбора информации о коммутаторе, необходимой инженерам для устранения неполадок или анализа проблемы.

Пример

В данном примере показано, как отобразить информацию о технической поддержке всех модулей.

```
Switch#debug show tech-support

#------------------------------------------------------------------------------
#               DGS-1510-28XMP Gigabit Ethernet SmartPro Switch
#                        Technical Support Information
#
#                           Firmware: Build 1.70.005
#    Copyright(C) 2020  D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------------


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

[SYS 2000-1-1 00:04:52]

Boot Time           : 1 Jan 2000  00:00:00
RTC Time            : 2000/01/01 00:04:52
Boot PROM Version   : Build 1.00.016
Firmware Version    : Build 1.70.005
Hardware Version    : A1
Serial number       : RZNV1F1000011
MAC Address         : 3C-1E-04-A1-B9-E0
MAC Address Number  : 32

[STACKING 2000-1-1 00:04:52]
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

14-6 debug show cpu utilization

Данная команда используется для отображения полного коэффициента загрузки CPU, а также коэффициента загрузки CPU с разбивкой на процессы.

debug show cpu utilization

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы отобразить информацию по загрузке CPU и загрузке по каждому процессу.

Пример

В данном примере показано, как отобразить информацию о загрузке CPU с разбивкой на процессы.

```
Switch#debug show cpu utilization

Five seconds -   9 %         One minute -   9 %         Five minutes -   9 %

Process Name         5Sec     1Min     5Min
-----------------   ------   ------   ------
OS_UTIL              91 %     91 %     91 %
bcmCNTR.0             2 %      2 %      2 %
bcmLINK.0             2 %      2 %      2 %
bcmL2X.0              2 %      1 %      1 %
HISR0                 1 %      1 %      1 %

Switch#
```

14-7 debug show packet ports

Эта команда используется для отображения информации о статистике пакетов на портах SIO.

debug show packet ports unit [*UNIT-ID***] [sio1 | sio2]**

Параметры

UNIT-ID	(Опционально) Указывает идентификатор единицы стекирования.
sio1	(Опционально) Указывает для представления нижнего порта стекирования.
sio2	(Опционально) Указывает для представления более высокого порта стекирования.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте эту команду для отображения информации о статистике пакетов на портах SIO.

Пример

В данном примере показано, как отобразить информацию о порте SIO.

```
Switch#debug show packet ports unit 1 sio1

UNIT ID 1 SIO 1:
Frame Size/Type          Frame Counts                Frames/sec
---------------          ----------------------      -----------
rxHCTotalPkts            0                           0
rxHCUnicastPkts          0                           0
rxHCMulticastPkts        0                           0
rxHCBroadcastPkts        0                           0
rxHCOctets               0                           0
rxHCPkt64Octets          0                           0
rxHCPkt65to127Octets     0                           0
rxHCPkt128to255Octets    0                           0
rxHCPkt256to511Octets    0                           0
rxHCPkt512to1023Octets   0                           0
rxHCPkt1024to1518Octets  0                           0
rxHCPkt1519to2047Octets  0                           0
rxHCPkt2048to4095Octets  0                           0
rxHCPkt4096to9216Octets  0                           0
txHCTotalPkts            0                           0
txHCUnicastPkts          0                           0
txHCMulticastPkts        0                           0
txHCBroadcastPkts        0                           0
txHCOctets               0                           0
txHCPkt64Octets          0                           0
txHCPkt65to127Octets     0                           0
txHCPkt128to255Octets    0                           0
txHCPkt256to511Octets    0                           0
txHCPkt512to1023Octets   0                           0
txHCPkt1024to1518Octets  0                           0
txHCPkt1519to2047Octets  0                           0
txHCPkt2048to4095Octets  0                           0
rxHCPkt4096to9216Octets  0                           0

Switch#
```

14-8 debug show error ports unit

Эта команда используется для отображения статистической информации об ошибках портов SIO.

debug show error ports unit [*UNIT-ID]* **[sio1 | sio2]**

Параметры

UNIT-ID	(Опционально) Указывает идентификатор единицы стекирования.

sio1	(Опционально) Указывает для представления нижнего порта стекирования.
sio2	(Опционально) Указывает для представления более высокого порта стекирования.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте эту команду для отображения информации о статистике ошибок портов SIO.

Пример

В этом примере показано, как отобразить информацию о статистике ошибок портов SIO.

```
Switch#debug show error ports unit 1 sio1

UNIT ID 1 SIO 1:
                    RX Frames                          TX Frames
                    ---------                          ---------
CRC Error           0             CRC Error            0
Undersize           0             STP Drop             0
Oversize            0             HOL Drop             0
Fragment            0             COS0 HOL Drop        0
Jabber              0             COS1 HOL Drop        0
Symbol Error        0             COS2 HOL Drop        0
Buffer Full Drop    0             COS3 HOL Drop        0
ACL Drop            0             COS4 HOL Drop        0
Multicast Drop      0             COS5 HOL Drop        0
VLAN Ingress Drop   0             COS6 HOL Drop        0
Invalid IPv6 Drop   0             COS7 HOL Drop        0
STP Drop            0
Storm and FDB Drop  0
MTU Drop            0

Switch#
```

15. Команды DHCP Auto-Configuration

15-1 autoconfig enable

Данная команда используется для включения функции автоконфигурации. Используйте форму **no**, чтобы отключить данную функцию.

autoconfig enable
no autoconfig enable

Параметры

Нет

По умолчанию

По умолчанию данная функция выключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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-серверзапущен 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)#
```

15-2 show autoconfig

Данная команда используется для отображения статуса автоконфигурации.

show autoconfig

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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#
```

16. Команды DHCP Client

16-1 ip dhcp client class-id

Данная команда используется для обозначения Vendor Class Identifier, используемого в качестве значения Option 60 для сообщения DHCP Discover. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Параметры

STRING	Укажите Vendor Class Identifier в формате строки. Максимальная длина строки – 32 символа.
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

Уровень команды по умолчанию

Уровень 12

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 включить DHCP-клиент, запустить отправку Vendor Class Identifier и указать его значение. Указанное значение – VOIP-Device для VLAN 100.

```
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)#
```

16-2 ip dhcp client client-id

Данная команда используется для обозначения интерфейса VLAN, чей шестнадцатеричный MAC-адрес будет использован в качестве ID клиента, отправляемого в сообщении Discover. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Параметры

INTERFACE-ID	Укажите интерфейс VLAN, чей шестнадцатеричный MAC-адрес 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

Уровень команды по умолчанию

Уровень 12

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)#
```

16-3 ip dhcp client hostname

Используйте данную команду, чтобы указать значение опции имени узла (Host Name) для отправки в сообщении DHCP Discover. Используйте форму no, чтобы вернуться к настройкам по умолчанию.

ip dhcp client hostname *HOST-NAME*
no ip dhcp client hostname

Параметры

HOST-NAME	Укажите имя узла. Максимальная длина строки – 64 символа. Имя узла должно начинаться с буквы, заканчиваться буквой или точкой,внутри можно использовать буквы, точки и дефисы.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать строку имени узла (Option 12) для отправки в сообщении DHCP Discover. Данная функция применяется только для последующей отправки сообщений DHCP Discover. Данная функция работает, когда на интерфейсе включен DHCP-клиент, который может получить IP-адрес от DHCP-сервера. Если данная функция не настроена, коммутатор будет отправлять сообщения без Option 12.

Пример

В данном примере показано, как установить значение опции имени узла (Host Name). Указанное значение – Site-A-Switch.

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

16-4 ip dhcp client lease

Данная команда используется для указания времени аренды IP-адреса, который необходимо запросить у DHCP-сервера. Используйте форму **no**, чтобы отключить данную функцию.

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

Уровень команды по умолчанию

Уровень 12

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)#
```

17. Команды DHCP Relay

17-1 class (DHCP Relay)

Эта команда используется для входа в режим конфигурации пула DHCP и ассоциации диапазона IP-адресов с классом DHCP. Для удаления ассоциации используйте форму **no** этой команды.

class *NAME*
no class *NAME*

Параметры

NAME	Указывает имя класса DHCP с максимальным количеством символов 32.

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для связывания пула ретрансляции DHCP с классом пула DHCP. Используйте команду **relay target** для определения списка целевых адресов ретрансляции для пересылки пакетов DHCP. Если запрос клиента DHCP соответствует пулу ретрансляции, который настроен с классами, клиент должен соответствовать классу, настроенному в пуле, чтобы быть переданным. Если класс DHCP не настроен, запрос будет сопоставлен только с пулом ретрансляции и будет передан на сервер назначения ретрансляции, указанный для сопоставленного пула ретрансляции.

Пример

В этом примере показано, как настроить класс DHCP "Service-A", определенный с шаблоном соответствия DHCP Option 60 0x112233 и 0x102030, отнесенный к пулу ретрансляции "pool1" и связанный с целью ретрансляции "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)#
```

17-2 ip dhcp class (DHCP Relay)

Эта команда используется для определения класса DHCP и входа в режим конфигурации класса DHCP. Для удаления класса DHCP используйте форму **no** этой команды.

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

Параметры

NAME	Указывает имя класса DHCP с максимальным количеством символов 32.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для входа в режим конфигурации класса DHCP. В этом режиме пользователь может использовать команду **option hex** для определения шаблона сопоставления опций для класса DHCP. Если класс не имеет связанной с ним опции option hex, класс будет соответствовать любому пакету.

Пример

В этом примере показано, как настроить класс DHCP "Service-A" и определить его с помощью шаблона соответствия DHCP Option 60 0x112233.

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

17-3 ip dhcp pool (DHCP Relay)

Данная команда используется для настройки пула DHCP Relay на DHCP Relay Agent, а также для входа в режим настройки пула DHCP. Используйте форму **no**, чтобы удалить пул DHCP-Relay.

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

Параметры

NAME	Укажите имя пула адресов. Максимально допустимое количество символов – 32.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Наряду с пакетами DHCP Relay, подчиняющимися команде **ip helper-address**, Relay Destination DHCP-сервера можно указать в пуле DHCP Relay. Для этого войдите в режим настройки пула DHCPпри 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.

Если подсеть, от которой приходит пакет DHCP-запроса, соответствует Relay Source Relay-пула, пакет будет ретранслирован на основе данного пула. В других случаях пакет ретранслируется на основе IP Helper-адреса, настроенного для получающего интерфейса. 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**, чтобыопределить 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)#
```

17-4 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. Используйте форму **no** для общего отключения функции Check для Option 82.

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

Уровень команды по умолчанию

Уровень 12

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 функция Check отключена, пакет будет передан напрямую.

Пример

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

```
Switch# configure terminal
Switch(config)# ip dhcp relay information check
Switch(config)#
```

17-5 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. Используйте форму **no**, чтобы удалить данные настройки для интерфейса.

ip dhcp relay information check-reply [none]
no ip dhcp relay information check-reply

Параметры

none	(Опционально) Укажите, чтобы отключить функцию Check для Option 82 ответного пакета.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 отключить общую 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
Switch(config-if)#
```

17-6 ip dhcp relay information option

Данная команда используется для того, чтобы включить вставку информации о Relay Agent (Option 82) в ретранслируемых пакетах DHCP-запроса. Используйте форму **no**, чтобы отключить данную функцию.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применима, если запущена команда **service dhcp**.

Если Option 82 DHCP запущена, в пакет DHCP, получаемый от клиента, будет встроено поле Option 82 перед ретрансляцией на сервер. Option 82 DHCP содержит две sub-опции: Circuit ID и Remote ID.

Команда **ip dhcp relay information option remote-id** используется для указания строки, задаваемой 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)#
```

17-7 ip dhcp relay information option-insert

Данная команда используется для включения/выключения встраивания Option 82 для интерфейса в ретранслируемые пакеты DHCP-запроса. Используйте форму **no**, чтобы удалить настройки данной функции для интерфейса.

ip dhcp relay information option-insert [none]
no ip dhcp relay information option-insert

Параметры

none	(Опционально) Укажите, чтобы отключить встраивание Option 82 в ретранслируемый пакет.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применима, если запущена команда **service dhcp**.

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)#
```

17-8 ip dhcp relay information policy

Данная команда используется для настройки алгоритма перенаправления Option 82 для DHCP Relay Agent. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда вступает в силу, когда включена команда **service dhcp**.

Используйте данную команду для настройки общего алгоритма встраивания Option 82 в пакеты, уже имеющие Option 82.

Пример

В этом примере показано, как настроить политику повторной переадресации опций агента ретрансляции на сохранение.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information policy keep
Switch(config)#
```

17-9 ip dhcp relay information policy-action

Данная команда используется для настройки алгоритма перенаправления Option 82 для DHCP Relay Agent на интерфейсе. Используйте форму **no**, чтобы удалить настройки.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применима, если запущен сервис DHCP. Используйте данную команду, чтобы настроить алгоритм встраивания Option 82 на интерфейсе в пакеты, у которых уже есть Option 82.

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)#
```

17-10 ip dhcp relay information option format remote-id

Эта команда используется для настройки подварианта удаленного ID информации DHCP. Используйте форму **no** этой команды для настройки подпараметра удаленного ID по умолчанию.

ip dhcp relay information option format remote-id {default| string *STRING* **| vendor2 | vendor3 | expert-udf [standalone_unit_format {0 | 1}]}**
no ip dhcp relay information option format remote-id

Параметры

default	Указывает на использование системного MAC-адреса коммутатора в качестве удаленного идентификатора.
string *STRING*	Указывает на использование заданной пользователем строки в качестве удаленного идентификатора. В строке допускаются пробельные символы.
vendor2	Указывает на использование поставщика 2.
vendor3	Указывает на использование поставщика 3.
expert-udf	Указывает на использование expert-udf.
standalone_unit_format	Указывает идентификатор устройства для автономного устройства. Значение по умолчанию равно 0.

По умолчанию

В качестве строки удаленного идентификатора используется системный MAC-адрес коммутатора.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format remote-id vendor2
Switch(config)#
```

В данном примере 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)#
```

17-11 ip dhcp relay information option format-type remote-id

Эта команда используется для настройки подварианта удаленного ID информации DHCP в строке формата поставщика в режиме конфигурации интерфейса. Используйте форму **no** этой команды, чтобы удалить подвариант удаленного ID строки формата поставщика.

ip dhcp relay information option format-type remote-id {vendor3 string *STRING* **| expert-udf** *NAME***}**
no ip dhcp relay information option format-type remote-id

Параметры

STRING	Указывает пользовательскую строку.
NAME	Указывает имя профиля.
vendor3	Указывает пользовательскую строку vendor 3 с максимальным количеством символов 32.
expert-udf	Указывает удаленный ID конкретных портов для связывания с конкретным профилем Option 82, максимум 32 символа.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применима для настройки интерфейсов физического порта и интерфейсов port-channel. Используйте данную команду для настройки строки, определенной как vendor для sub-опции Remote ID Option 82 на интерфейсе.

Пример

В этом примере показано, как определить строку формата vendor3 remote-id как "switch1" на порту 3.

```
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)#
```

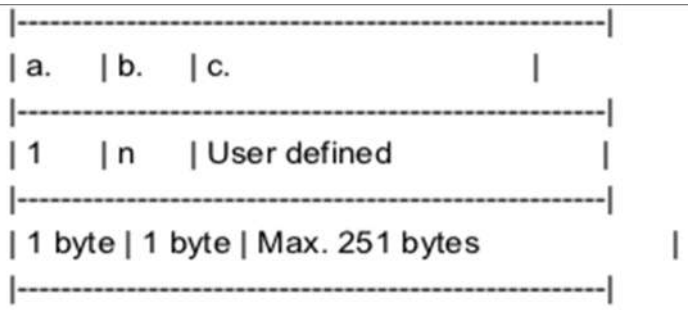
17-12 ip dhcp relay information option format circuit-id

Эта команда используется для настройки подварианта ID схемы информации DHCP. Используйте форму **no** этой команды для настройки подпараметра ID цепи по умолчанию.

ip dhcp relay information option format circuit-id {default | string *STRING* **| vendor1 | vendor2 | vendor3 | vendor4 | vendor5 | vendor6 | expert-udf [standalone_unit_format {0|1}]}**
no ip dhcp relay information option format circuit-id

Параметры

default	Указывает на использование подварианта ID схемы по умолчанию.
string *STRING*	Указывает на использование заданной пользователем строки в качестве идентификатора цепи. В строке допускаются пробельные символы.
vendor1	Указывает использовать vender1.
vendor2	Указывает использовать vender2.
vendor3	Указывает использовать vender3.
vendor4	Указывает использовать vender4.
vendor5	Указывает использовать vender5.
vendor6	Указывает использовать vender6.
expert-udf	Указывает использовать expert-udf. Если настроено, используйте заданную пользователем строку в качестве идентификатора схемы:



a.	b.	c.
1	n	User defined
1 byte	1 byte	Max. 251 bytes

a. Тип подварианта: Число 1 указывает на то, что это идентификатор цепи.

b. Длина: Общая длина определяемой пользователем строки. По умолчанию Length равна 0 и поле значений отсутствует.

c. Значение: Гибкая определяемая пользователем строка, которая конфигурируется с помощью этой команды и команды **ip dhcp relay information profile**. Максимальная длина - 251.

По умолчанию

Формат идентификатора цепи: идентификатор VLAN, номер модуля и номер порта.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 данном примере 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)#
```

17-13 ip dhcp relay information option format-type circuit-id

Эта команда используется для настройки подварианта ID информационной схемы DHCP в строке, определяемой пользователем.

ip dhcp relay information option format-type circuit-id {vendor3 string *STRING* **| expert-udf** *NAME***}**
no ip dhcp relay information option format-type circuit-id

Параметры

STRING	Указывает строку, определяемую поставщиком.
NAME	Указывает имя профиля.
vendor3	Указывает на пользовательскую строку vender3, содержащую не более 32 символов.
expert-udf	Указывает идентификатор цепи конкретных портов для связывания с конкретным профилем Option 82, максимум 32 символа.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и интерфейсов port-channel. Используйте данную команду для настройки строки, определенной как vendor для sub-опции Circuit ID Option 82 на интерфейсе.

Пример

В этом примере показано, как определить vendor3 circuit-id "abc" на порту 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)#
```

17-14 ip dhcp relay information trust-all

Данная команда позволяет назначить на DHCP Relay Agent все интерфейсы, отправляющие информацию об IP DHCP Relay, доверенными. Используйте форму **no**, чтобы отключить функцию Trust для всех интерфейсов.

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

Уровень команды по умолчанию

Уровень 12

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. Информация Relay считается доверенной со всехинтерфейсов, вне зависимости от настроек команды **ip dhcp relay information trusted**.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information trust-all
Switch(config)#
```

17-15 ip dhcp relay information trusted

Данная команда позволяет назначить на DHCP Relay Agent определенный интерфейс, отправляющий информацию об IP DHCP Relay, в качестве доверенного. Используйте форму **no**, чтобы отключить функцию Trust для интерфейса.

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

Уровень команды по умолчанию

Уровень 12

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 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 на DHCP Relay Agent снять статус Trust для всех интерфейсов 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)#
```

17-16 ip dhcp local-relay vlan

Данная команда используется для включения Local Relay на одной из VLAN или группе VLAN. Используйте форму **no**, чтобы отключить данную функцию.

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 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Local Relay обеспечивает передачу сообщения DHCP на все локальные порты-участники 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)#
```

17-17 ip dhcp smart-relay

Эта команда используется для включения функции интеллектуальной ретрансляции агента ретрансляции DHCP. Используйте форму **no** этой команды для отключения функции интеллектуальной эстафеты.

ip dhcp smart-relay
no ip dhcp smart-relay

Параметры

Нет

По умолчанию

По умолчанию эта опция отключена

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если полученный интерфейс пакета имеет вторичные адреса, по умолчанию агент ретрансляции устанавливает в поле адреса шлюза пакета первичный адрес интерфейса. Если включена интеллектуальная ретрансляция, агент ретрансляции будет подсчитывать количество повторных попыток отправки клиентом сообщения DISCOVER. После трех повторных попыток агент ретрансляции изменит адрес шлюза на вторичный адрес полученного интерфейса.

Пример

В этом примере показано, как включить функцию интеллектуального реле.

```
Switch# configure terminal
Switch(config)# ip dhcp smart-relay
Switch(config)#
```

17-18 option hex (DHCP Relay)

Эта команда используется для указания шаблона соответствия опций DHCP для класса DHCP. Используйте форму **no** этой команды для удаления указанного шаблона соответствия для класса DHCP.

option *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**
no option *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**

Параметры

CODE	Указывает номер опции DHCP.
PATTERN	Указывает шестнадцатеричный шаблон указанного параметра DHCP.
*	(Опционально) Указывает не сопоставлять оставшиеся биты параметра. Если не указано, длина бита *PATTERN* должна быть равна такой же, как длина бита опции.
MASK	(Опционально) Указывает шестнадцатеричную битовую маску для маскирования шаблона. Будут проверяться маскированные биты шаблона. Если не указано, будут проверены все биты, указанные в PATTERN. Бит, установленный в FF, будет проверен. Формат ввода должен быть таким же, как и у PATTERN.

По умолчанию

Нет

Режим ввода команды

DHCP Class Configuration Mode.

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду **ip dhcp class** вместе с этой командой для определения класса DHCP. Классы в пуле

сопоставляются в последовательности конфигурации классов в пуле.

С помощью команды **option hex** пользователь может указать номер кода опции DHCP с его шаблоном сопоставления для класса DHCP. Для класса DHCP можно указать несколько шаблонов опций. Если пакет соответствует любому из указанных шаблонов класса DHCP, пакет будет отнесен к классу DHCP и перенаправлен в соответствии с указанной целью.

Ниже перечислены некоторые часто используемые коды опций:

- Option 60: идентификатор класса поставщика.
- Option 61: идентификатор клиента.
- Option 77: класс пользователя.
- Option 124: класс поставщика, идентифицирующий поставщика.
- Option 125: информация, идентифицирующая конкретного поставщика.

Пример

В этом примере показано, как настроить класс DHCP "Service-A" для определения с помощью DHCP Option 60 шаблона соответствия 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)#
```

17-19 relay destination

Данная команда используется для указания IP-адреса DHCP Relay Destination, ассоциированного с Relay-пулом. Используйте форму **no**, чтобы удалить Relay Destination из пула DHCP-Relay.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Наряду с пакетами DHCP Relay, подчиняющимися команде **ip helper-address**, Relay Destination DHCP-сервера можно указать в пуле DHCP Relay. Для этого войдите в режим настройки пула DHCPпри 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 Relay Sources и несколько Relay Destinations. Если пакет соответствует какому-либо из Relay Sources, он будет отправлен на всеRelay Destinations.

Если подсеть, от которой приходит пакет DHCP-запроса, соответствует Relay Source Relay-пула, пакет будет ретранслирован на основе данного пула. В других случаях пакет ретранслируется на основе IP Helper-адреса, настроенного для получающего интерфейса. 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**, чтобысвязать 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)#
```

17-20 relay source

Данная команда используется для указания подсети-источника (source) пакетов клиента. Используйте форму **no**, чтобы удалить подсеть-источник (source).

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Наряду с пакетами DHCP Relay, подчиняющимися команде **ip helper-address**, 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 Relay Sources и несколько
Relay Destinations. Если пакет соответствует какому-либо из Relay Sources, он будет отправлен на все Relay Destinations.

При получении пакета DHCP-запроса, если подсеть полученного пакета соответствует Relay Source

Relay-пула, пакет будет ретранслирован на основе данного пула. В других случаях пакет ретранслируется на основе IP Helper-адреса, настроенного для получающего интерфейса. 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 «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)#
```

17-21 relay target

Данная команда используется для указания DHCP Relay Target для ретранслируемых пакетов, которая соответствует шаблону значений опции, установленной в классе. Используйте форму **no**,чтобы удалить Relay Target.

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 Class Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

В пуле DHCP Relay 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)#
```

17-22 service dhcp (DHCP Relay)

Эта команда используется для включения службы ретрансляции DHCP на коммутаторе. Используйте форму **no** этой команды для отключения службы ретрансляции DHCP.

service dhcp
no service dhcp

Параметры

Нет

По умолчанию

По умолчанию эта опция отключена

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для включения или отключения службы ретрансляции DHCP на коммутаторе.

Пример

В этом примере показано, как отключить службу ретрансляции DHCP.

```
Switch#configure terminal
Switch(config)#no service dhcp
Switch(config)#
```

17-23 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду для отображения рабочих настроек функции Trust Relay Option.

Пример

В этом примере показано, как отобразить эффективную настройку функции опции trust relay information, 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:
vlan 100            vlan 200            vlan 300            vlan 400
vlan 500

Total Entries: 5

Switch#
```

В этом примере показано, как отобразить эффективную настройку функции опции trust relay information, 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#
```

17-24 show ip dhcp relay information option-insert

Эта команда используется для отображения конфигурации вставки опции relay.

show ip dhcp relay information option-insert

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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
------------ ----------
vlan 1         Enabled
vlan 2         Disabled
vlan 3         Not Configured

Total Entries: 3

Switch#
```

17-25 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-ID	(Опционально) Укажите для отображения информации об интерфейсе. Введите ID интерфейса после ключевого слова. Если ID интерфейса не указан, будет отображена информация обо всех интерфейсах.
,	(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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения настроек формата опций интерфейса.

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#
```

17-26 show ip dhcp relay information policy-action

Данная команда используется для отображения информации об алгоритме перенаправления Relay Option для интерфейса.

show ip dhcp relay information policy-action

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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
-------------- ----------
vlan 1          Keep
vlan 2          Drop
vlan 3          Replace
vlan 4          Not configured

Total Entries: 3

Switch#
```

17-27 ip dhcp relay information profile

Данная команда используется для того, чтобы задать профиль Option 82 и входа в режим Profile Configure Option 82. Используйте форму **no**, чтобы удалить указанный профиль Option 82.

ip dhcp relay information profile *PROFILE-NAME*
no ip dhcp relay information profile *PROFILE-NAME*

Параметры

PROFILE-NAME	Укажите имя профиля для определения профиля Option 82. Максимально допустимое количество символов – 32.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для входа в режим Profile Configure Option 82, чтобы задать профиль Option 82. При помощи профиля можно самостоятельно задать произвольную запись Option 82.

Пример

В данном примере показано, как войти в режим Profile Configure Option 82, чтобы задать профиль «remote_id».

```
Switch#configure terminal
Switch(config)#service dhcp
Switch(config)#ip dhcp relay information profile remote_id
Switch(config-dhcp-profile)#
```

17-28 format string

Данная команда используется для создания произвольной записи Option 82. Используйте форму **no**, чтобы удалить запись.

format string *FORMAT-STRING*
no format string

Параметры

FORMAT-STRING	Укажите формат Option 82 DHCP. 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, которуюнеобходимо преобразовать до того, как она будет запакетирована. 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. Даннаяопция 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**). Заполнениеначального нуля – настройка по умолчанию. **1-32** – (опционально) индикатор длины. Данная опция указывает, сколько символов или байтов должна занимать преобразованная ключевая строка. Если фактическая длина транслируемой ключевой строки меньше длины, предусмотренной данной опцией, будет ипользован индикатор заполнения. В других случаях будет использована фактическая длина строки. **keyword -**ключевое слово будет преобразовано на основе фактического значения системы. Следующие ключевые слова указывают, что команда будет отклонена при обнаружении неизвестных или неподдерживаемых ключевых слов: **devtype:** модель устройства. Выводится из поля Module Name в команде **show version**. Допустимо использование только строки ASCII.

sysname: системное имя коммутатора. Максимально допустимое количество символов – 128. Допустимоиспользование только строки ASCII.

ifdescr: выводится из ifDescr (IF-MIB). Допустимо использование только строки ASCII.

portmac: MAC-адрес порта. Могут быть использованы строка ASCII или шестнадцатеричныезначения. При использовании строки ASCII MAC-адрес может быть настроен с помощью специальной команды (например, **ip dhcp relayinformation 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 шестнадцатеричныезначения. При использовании строки ASCII MAC-адрес может быть сформирован при помощикоманд CLI (например, **ip dhcp relay information option mac-format case**). При использовании шестнадцатеричных символов MAC-адрес будет сформирован в шестнадцатеричном виде.

unit: Unit ID коммутатора в стеке. Могут быть использованы строка ASCII или шестнадцатеричныезначения. Для нестекированных коммутаторов ID указывается при помощи команды **ip dhcp relay information option format remote-id expert-udf [standalone_unit_format {0 | 1}]**, а также команды **ipdhcp relay information option format circuit-id expert-udf [standalone_unit_format {0 | 1}]**.

module: ID модуля. Могут быть использованы строкаASCII или шестнадцатеричные значения.

port: номер локального порта. Могут быть использованы строка ASCII или шестнадцатеричныезначения.

svlan: ID внешней VLAN. Могут быть использованы строка ASCII или шестнадцатеричные значения.
cvlan: ID внутренней VLAN. Могут быть использованы строка ASCII или шестнадцатеричныезначения.

: - 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 знакаперехода. Специальные символы после **** являются самостоятельными символами. Например, **%** в комбинации **\%** является самостоятельным символом, ане индикатором запуска отформатированной ключевойстроки. Пробелы вне отформатированной ключевой строки также будут включены. • Шестнадцатеричные значения могут содержать любыекомбинации отформатированных ключевых строк, символов 0-9, A-F, a-f и пробелов. Отформатированныеключевые 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

DHCP Profile Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для настройки записи Option 82, заданной пользователем.

Пример

В данном примере показано, как настроить запись Option 82, заданную пользователем.

```
Switch#configure terminal
switch(config)# ip dhcp relay information profile profile1
switch(config-dhcp-profile)#format string Ethernet "%unit:"/0/
"%port:"\:%sysname:"%05svlan
switch(config-dhcp-profile)#
```

17-29 ip dhcp relay information option mac-format case

Данная команда используется для настройки формата MAC-адреса, задаваемого пользователем в профиле Option 82. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ip dhcp relay information option mac-format case {lowercase | uppercase} delimiter {hyphen |colon | dot | none } number {1 | 2 | 5}

no ip dhcp relay information option mac-format case

Параметры

lowercase	Укажите, чтобы использовать нижний регистр при записи MAC-адреса Option 82 для задаваемого пользователем профиля: aa-bb-cc-dd-ee-ff.
uppercase	Укажите, чтобы использовать верхний регистр при записи MAC-адреса Option 82 для задаваемого пользователем профиля: 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:** несколько 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки формата MAC-адреса, заданного пользователем в профиле Option 82.

Пример

В данном примере показано, как настроить формат MAC-адреса, заданного пользователем в профиле Option 82.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information option mac-format case uppercase delimiter hyphen
number 5
Switch(config)#
```

17-30 show ip dhcp relay information profile

Данная команда используется для отображения настройки профиля Option 82 DHCP.

show ip dhcp relay information profile [*PROFILE-NAME***]**

Параметры

PROFILE-NAME	(Опционально) Укажите, чтобы отобразить имя профиля Option 82.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения настройки профиля Option 82 DHCP.

Пример

В данном примере показано, как отобразить настройки профиля Option 82 DHCP.

```
Switch# show ip dhcp relay information profile

Profile name: profile1
Format string: "Ethernet %unit:/0/  %port:\:%sysname:%05svlan"

Profile name: profile2
Format string: "Ethernet "%unit:"/0/  "%port:"\:%sysname:"%05svlan

Total Entries: 2

Switch#
```

17-31 show ip dhcp relay information option mac-format

Данная команда используется для отображения формата MAC-адреса в профиле Option 82.

show ip dhcp relay information option mac-format

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения формата MAC-адреса в профиле Option 82.

Пример

В данном примере показано, как отобразить формат MAC-адреса в профиле Option 82.

```
Switch#show ip dhcp relay information option mac-format

 Case              : Uppercase
 Delimiter         : Hyphen
 Delimiter Number  : 5
 Example           : AA-BB-CC-DD-EE-FF

Switch#
```

18. Команды DHCP Server

18-1address range

Данная команда используется для обозначения диапазона IP-адресов, которые необходимо ассоциировать с DHCP-классом в пуле DHCP-адресов. Используйте форму **no** для удаления диапазона адресов, которые необходимо ассоциировать с DHCP-классом.

address range *START-IP-ADDRESS END-IP-ADDRESS*
no address range *START-IP-ADDRESS END-IP-ADDRESS*

Параметры

START-IP-ADDRESS	Укажите адрес или первый адрес в диапазоне адресов.
END-IP-ADDRESS	Укажите последний адрес в диапазоне адресов.

По умолчанию

Нет

Режим ввода команды

DHCP Pool Class Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команды **address range** и **class** в конфигурации пула DHCP используются для того, чтобы ограничить выделение IP-адресов из подсети. Сеть разбивается на разделы на основе значения опции DHCP- запроса. Если в пуле адресов определены классы, то назначение адреса будет основано на классе этого адресного пула.

Когда сервер пытается выделить адрес из пула адресов, и если у пула определены классы, то сервер сначала проверит, содержит ли пул запрашиваемую подсеть. Если подсеть пула адресов содержит GIADDR (не равно нулю) или подсеть принимаемого интерфейса, то сервер будет выделять из пула адрес, соответствующий определенному классу.

Для удаления диапазона адресов можно указать только точный диапазон адресов, который уже был ранее настроен.

Пример

В данном примере показано, как создать DHCP-класс «Customer-A» с шаблоном, соответствующим Relay Information Option (Option 82). Он ассоциирован с диапазоном адресов DHCP «pool1».

```
Switch# configure terminal
Switch(config)# ip dhcp class Customer-A
Switch(config-dhcp-class)# option 82 hex 1234 *
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# network 172.28.5.0/24
Switch(config-dhcp-pool)# class Customer-A
Switch(config-dhcp-pool-class)# address range 172.28.5.1 172.28.5.12
witch(config-dhcp-pool-class)#
```

18-2 bootfile

Используйте данную команду, чтобы указать файл конфигурации или файл образа для загрузки на устройство DHCP-клиента. Используйте форму **no**, чтобы удалить загрузочный файл.

bootfile *URL*
no bootfile

Параметры

URL	Укажите ссылку на файл загрузки. Максимально допустимая длина ссылки – 64 символа.

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать файл конфигурации или файл образа для загрузки на устройство DHCP-клиента. Команда **next-server** указывает местоположение сервера, на котором находится загрузочный файл.

Пример

В данном примере показано, как указать файл «mdubootfile.bin» для DHCP-пула «pool1» в качестве загрузочного.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# bootfile \bootimage\mdubootfile.bin
Switch(config-dhcp-pool)#
```

18-3 clear ip dhcp binding

Данная команда используется для удаления записи привязки адресов из базы данных DHCP-сервера.

clear ip dhcp {all | pool *NAME***} binding {* | *IP-ADDRESS*}**

Параметры

all	Укажите, чтобы очистить записи привязки всех пулов.
pool *NAME*	Укажите имя DHCP-пула.
*	Укажите, чтобы очистить все записи привязки, ассоциированные с указанным пулом.
IP-ADDRESS	Укажите IP-адрес записи привязки, которую необходимо удалить.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для удаления привязок адресов. Если задан параметр **pool**, а значение IP-адреса – *, то все автоматические записи привязок, ассоциированные с пулом, будут удалены.
Если значение параметра **pool** – all, и IP-адрес указан, то автоматическая запись привязки, относящаяся к IP-адресу, будет удалена независимо от пула, в котором содержится запись привязки. Если указаны и параметр **pool**, и IP-адрес, автоматическая запись указанного IP-адреса в обозначенном пуле будет удалена.

Пример

В данном примере показано, как удалить привязку адреса 10.12.1.99 из базы данных DHCP-сервера.

```
Switch# clear ip dhcp all binding 10.12.1.99
Switch#
```

В данном примере показано, как удалить все привязки изо всех пулов.

```
Switch# clear ip dhcp all binding *
Switch#
```

В данном примере показано, как удалить привязку адреса 10.13.2.99 из пула адресов pool2.

```
Switch# clear ip dhcp pool pool2 binding 10.13.2.99
Switch#
```

18-4 clear ip dhcp conflict

Данная команда используется для удаления записи конфликта DHCP из базы данных DHCP-сервера.

clear ip dhcp {all | pool *NAME***} conflict {* | *IP-ADDRESS*}**

Параметры

all	Укажите, чтобы удалить записи конфликтов для всех пулов.
pool *NAME*	Укажите имя DHCP-пула.
*	Укажите, чтобы удалить все записи конфликтов, ассоциированные с указанным пулом.
IP-ADDRESS	Укажите IP-адрес записи конфликта, которую необходимо.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для удаления адреса из таблицы конфликтов. Удаленный адрес будет возвращен в пул адресов и может быть использован в дальнейшем. DHCP-сервер обнаруживает конфликт IP-адреса при помощи операции Ping.

Если задан параметр **pool**, а значение IP-адреса – *, то все записи конфликта, относящиеся к пулу, будут удалены. Если значение параметра **pool** – all, и IP-адрес указан, то указанная запись конфликта будет удалена независимо от пула, в котором содержится запись конфликта. Если указаны и параметр **pool**, и IP-адрес, то обозначенная запись конфликта в соответствующем пуле будет удалена.

Пример

В данном примере показано, как удалить конфликт с адресом 10.12.1.99 из базы данных DHCP-сервера.

```
Switch# clear ip dhcp all conflict 10.12.1.99
Switch#
```

В данном примере показано, как удалить все адресные конфликты из базы данных DHCP-сервера.

```
Switch# clear ip dhcp all conflict *
Switch#
```

В данном примере показано, как удалить все адресные конфликты из пула адресов pool1.

```
Switch# clear ip dhcp pool pool1 conflict *
Switch#
```

В данном примере показано, как удалить конфликт с адресом 10.13.2.99 из пула адресов pool2.

```
Switch# clear ip dhcp pool pool2 conflict 10.13.2.99
Switch#
```

18-5 clear ip dhcp server statistics

Данная команда используется для сброса всех счетчиков DHCP-сервера.

clear ip dhcp server statistics

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для сброса всех счетчиков статистики DHCP.

Пример

В данном примере показано, как обнулить все счетчики DHCP.

```
Switch# clear ip dhcp server statistics
Switch#
```

18-6 class (DHCP Server)

Эта команда используется для привязки диапазона IP-адресов к классу DHCP. Используйте форму **no** этой команды, чтобы удалить ассоциацию.

class *NAME*
no class *NAME*

Параметры

NAME	Укажите имя DHCP-класса. Максимально допустимое количество символов – 32.

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду **address range** и эту команду в пуле адресов DHCP для ограничения выделения IP-адреса из подсети в пуле адресов. Сеть для выделения адресов разделяется на основе значения опции DHCP запроса. Если в адресном пуле определены классы, распределение адресов будет основано на классе из этого адресного пула, если включена команда **ip dhcp use class**.

Пример

В данном примере показано, как создать два DHCP-класса Customer-A и Customer-B с соответствующими шаблонами Option 82. Они ассоциированы с диапазонами адресов DHCP-сервера «srv-pool1».

```
Switch# configure terminal
Switch(config)# ip dhcp class Customer-A
Switch(config-dhcp-class)# option 82 hex 1234 *
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp class Customer-B
Switch(config-dhcp-class)# option 82 hex 5678 *
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp pool srv-pool1
Switch(config-dhcp-pool)# network 172.28.5.0/24
Switch(config-dhcp-pool)# class Customer-A
Switch(config-dhcp-pool-class)# address-range 172.28.5.1 172.28.5.12
witch(config-dhcp-pool-class)# exit
Switch(config-dhcp-pool)# class Customer-B
Switch(config-dhcp-pool-class)# address-range 172.28.5.18 172.28.5.32
Switch(config-dhcp-pool-class)#
```

В данном примере показано, как настроить DHCP-класс Service-A и задать соответствующий для него шаблон Option 60 DHCP 0x112233 и 0x102030. Другой класс Service-B настроен и задан с соответствующим ему шаблоном Option 60 DHCP 0x556677 и 0x506070. Класс Default-class настроен без опции. Эти заданные классы применяются в Relay-пуле «pool1». Класс Service-A ассоциирован с Relay Target 10.2.1.2, а класс Service-B ассоциирован с Relay Target 10.2.1.5. Класс Default-class ассоциирован с Relay Target 10.2.1.32.

```
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 class Service-B
Switch(config-dhcp-class)# option 60 hex 556677
Switch(config-dhcp-class)# option 60 hex 506070
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp class Default-class
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# relay source 172.19.18 255.255.255.0
Switch(config-dhcp-pool)# class Service-A
Switch(config-dhcp-pool-class)# relay target 10.2.1.2
Switch(config-dhcp-pool-class)# exit
Switch(config-dhcp-pool)# class Service-B
Switch(config-dhcp-pool-class)# relay target 10.2.1.5
Switch(config-dhcp-pool)# exit
Switch(config-dhcp-pool)# class Default-class
Switch(config-dhcp-pool-class)# relay target 10.2.1.32
Switch(config-dhcp-pool)#
```

18-7 client-identifier

Эта команда используется для указания уникального идентификатора клиента DHCP для записи ручной привязки в пуле адресов DHCP. Используйте форму **no** этой команды, чтобы удалить указание идентификатора клиента.

client-identifier *IDENTIFIER*
no client-identifier

Параметры

IDENTIFIER	Укажите идентификатор DHCP-клиента в шестнадцатеричном виде.

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда действительна для записей привязок, созданных вручную в пуле DHCP. Идентификатор клиента формируется по типу среды передачи и MAC-адреса. В пуле DHCP-адресов может быть указана

только одна запись привязки, созданная вручную. При вводе записи привязки IP-адрес может быть связан с ID клиента или с аппаратным адресом узла.

Используйте команды **client-identifier** и **host**, чтобы указать запись привязки, созданной вручную наоснове идентификатора клиента в DHCP-пакете.

Пример

В данном примере показано, как создать пул DHCP-адресов «pool1» с записью привязки, созданной вручную, которая связывает IP-адрес 10.1.2.3/24 с ID клиента 0x01524153203124.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# client-identifier 01524153203124
Switch(config-dhcp-pool)# host 10.1.2.3/24
Switch(config-dhcp-pool)#
```

18-8 default-router

Данная команда используется для указания шлюзов по умолчанию для DHCP-клиента. Используйте форму **no** для удаления шлюза по умолчанию.

default-router *IP-ADDRESS* **[***IP-ADDRESS2...IP-ADDRESS8***]**
no default-router *IP-ADDRESS* **[***IP-ADDRESS2...IP-ADDRESS8***]**

Параметры

IP-ADDRESS	Укажите IP-адрес шлюза по умолчанию для DHCP-клиента.
IP-ADDRESS2...IP-ADDRESS8	Укажите несколько IP-адресов, разделяя их при помощи пробелов. Максимально допустимое количество адресов – 8.

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки шлюза по умолчанию для клиента. IP-адрес шлюза должен принадлежать той же сети, что и подсеть клиента. Шлюзы перечислены в порядке приоритетности. Если шлюзы по умолчанию уже настроены, то шлюзы, настраиваемые позже, будут добавлены в список шлюзов по умолчанию.

Пример

В данном примере показано, как указать IP-адрес шлюза по умолчанию в пуле DHCP-адресов. Указанный IP-адрес – 10.1.1.1.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# default-router 10.1.1.1
```

18-9 domain-name

Данная команда используется для указания доменного имени для DHCP-клиента. Используйте форму **no** для удаления доменного имени.

domain-name *NAME*
no domain-name

Параметры

NAME	Укажите доменное имя. Максимально допустимое количествосимволов – 64.

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки доменного имени для DHCP-клиента. Можно указать не более одного доменного имени.

Пример

В данном примере показано, как указать доменное имя в пуле DHCP-адресов. Указанное доменное имя – «domain.com».

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# domain-name domain.com
```

18-10 dns-server

Данная команда используется для указания DNS-серверов для DHCP-клиента. Используйте форму **no** для удаления указанного DNS-сервера.

dns-server *IP-ADDRESS* **[***IP-ADDRESS2…IP-ADDRESS8***]**
no dns-server *IP-ADDRESS* **[***IP-ADDRESS2…IP-ADDRESS8***]**

Параметры

IP-ADDRESS	Укажите IP-адреса, которые будут использованы DHCP-клиентом в качестве DNS-сервера.
IP-ADDRESS2...IP-ADDRESS8	Укажите несколько IP-адресов, разделяя их при помощи пробелов. Максимально допустимое количествосерверов – 8.

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки IP-адреса, который будет использован клиентом в качестве DNS-сервера. Максимально допустимое количество серверов – 8. Серверы перечисляются в порядке приоритетности. Если DNS-серверы уже настроены, то серверы, настраиваемые позже, будут добавлены в список DNS-серверов.

Пример

В данном примере показано, как указать IP-адрес DNS-сервера в пуле DHCP-адресов. Указанный IP-адрес – 10.1.1.1.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# default-router 10.1.1.1
```

18-11 hardware-address

Эта команда используется для указания аппаратного адреса записи ручной привязки в пуле адресов DHCP. Используйте форму **no** этой команды, чтобы удалить указание аппаратного адреса записи ручной привязки.

hardware-address *HARDWARE-ADDRESS*
no hardware-address

Параметры

HARDWARE-ADDRESS	Укажите MAC-адрес клиента.

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Запись привязки — это сопоставление IP-адреса с аппаратным адресом оборудования или ID клиента. При создании записи привязки IP-адрес присваивается клиенту вручную.

В пуле DHCP-адресов может быть указано не более одной записи привязки. С помощью записи привязки IP-адрес может быть связан с идентификатором клиента или с аппаратным адресом узла.

Используйте команды **client-identifier** и **host**, чтобы настроить вручную запись привязки на основе идентификатора клиента в DHCP-пакете. Команды **hardware-address** и **host** используются для настройки вручную записи привязки на основе аппаратного адреса.

Пример

В данном примере показано, как создать пул DHCP-адресов с настроенной вручную записью привязки, которая связывает IP-адрес 10.1.2.100/24 с MAC-адресом C2:F3:22:0A:12:F4. Указанное имя пула – «pool1».

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# hardware-address C2F3.220A.12F4
Switch(config-dhcp-pool)# host 10.1.2.100/24
Switch(config-dhcp-pool)#
```

18-12 host

Данная команда используется для указания IP-адреса в настроенной вручную записи привязки пула DHCP-адресов. Используйте форму **no** для удаления IP-адреса из записи.

host {*IP-ADDRESS MASK* **|** *IP-ADDRESS***/** *PREFIX-LENGTH***}**
no host

Параметры

IP-ADDRESS	Укажите IP-адрес в настроенной вручную записи привязки.
MASK	Укажите биты, определяющие сетевую маску.
PREFIX-LENGTH	Укажите длину префикса сети. Это альтернативный способ указать сетевую маску.

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

В пуле DHCP-адресов может быть указано не более одной записи привязки. С помощью записи привязки IP-адрес может быть связан с идентификатором клиента или с аппаратным адресом узла.

Используйте команды **client-identifier** и **host** для настройки вручную записи привязки на основе идентификатора клиента. Команды **hardware-address** и **host** используются для настройки вручную записи привязки на основе аппаратного адреса.

Пример

В данном примере показано, как создать пул DHCP-адресов с настроенной вручную записью привязки, которая связывает IP-адрес 10.1.2.100/24 с MAC-адресом C2:F3:22:0A:12:F4. Указанное имя пула – «pool1».

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# hardware-address C2:F3:22:0A:12:F4
Switch(config-dhcp-pool)# host 10.1.2.100/24
Switch(config-dhcp-pool)#
```

18-13 ip dhcp class (DHCP Server)

Данная команда используется для настройки DHCP-класса и входа в режим конфигурации DHCP-класса. Используйте форму **no** для удаления DHCP-класса.

ip dhcp class NAME
no ip dhcp class NAME

Параметры

NAME	Укажите имя DHCP-класса. Максимально допустимое количество символов – 32.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для входа в режим конфигурации DHCP-класса. Затем при помощи команды **option hex** настройте соответствие шаблона опции с DHCP-классом. Если у класса отсутствует связка с шестнадцатеричной опцией, то классу будет соответствовать любой пакет.

Пример

В данном примере показано, как настроить DHCP-класс Service-A с соответствием шаблону 0x112233 Option 60 DHCP.

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

18-14 ip dhcp excluded-address

Данная команда используется для того, чтобы исключить диапазон IP-адресов для назначения клиенту. Используйте форму **no** для удаления исключенных адресов.

ip dhcp excluded-address *START-IP-ADDRESS END-IP-ADDRESS*
no ip dhcp excluded-address *START-IP-ADDRESS END-IP-ADDRESS*

Параметры

START-IP-ADDRESS	Укажите адрес или первый адрес диапазона адресов, которые необходимо исключить.
END-IP-ADDRESS	Укажите последний адрес диапазона адресов, которые необходимо исключить.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

DHCP-сервер автоматически распределяет адреса из пула DHCP-адресов по DHCP-клиентам. Для распределения доступны все адреса, кроме IP-адреса интерфейса шлюза и исключенных адресов,которые обозначены при помощи команды **ip dhcp excluded-address**. Можно отменить распределение нескольких диапазонов адресов. Для удаления диапазона исключенных адресов администратору необходимо указать точный диапазон данных адресов.

Пример

В данном примере показано, как исключить диапазон адресов. Указанный диапазон адресов: с 10.1.1.1 по 10.1.1.255 и с 10.2.1.1 по 10.2.1.255.

```
Switch# configure terminal
Switch(config)# ip dhcp excluded-address  10.1.1.1 10.1.1.255
Switch(config)# ip dhcp excluded-address  10.2.1.1 10.2.1.255
```

18-15 ip dhcp ping packets

Данная команда используется для указания количества пакетов, которое будет посылать DHCP-сервер в рамках Ping-операции. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ip dhcp ping packets *COUNT*
no ip dhcp ping packets

Параметры

COUNT	Укажите количество Ping-пакетов, которые будут отправленыDHCP-сервером.

По умолчанию

Значение по умолчанию – 2.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для указания количества пакетов, отправляемых DHCP-сервером в рамках Ping-операции. Ping-операция, выполняемая DHCP-сервером, позволяет определить наличие конфликта IP-адреса перед тем, как IP-адрес будет присвоен клиенту. При отсутствии ответа по истечении определенного количества попыток IP-адрес будет присвоен клиенту и занесен в запись. При получении сервером ответа на Ping-операцию IP-адрес будет занесен в запись конфликта.

Задайте 0, чтобы отключить Ping-операцию.

Пример

В данном примере показано, как указать количество Ping-пакетов. Указанное количество – 3.

```
Switch# configure terminal
Switch(config)# ip dhcp ping packets 3
Switch(config)#
```

18-16 ip dhcp ping timeout

Данная команда используется для указания времени ожидания ответного Ping-пакета DHCP-сервером. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ip dhcp ping timeout *MILLI-SECONDS*
no ip dhcp ping timeout

Параметры

MILLI-SECONDS	Укажите период ожидания ответного Ping-пакета DHCP-сервером. Максимальный период ожидания – 10000 миллисекунд (10 секунд). Указанное значение должно быть кратным 100.

По умолчанию

Значение по умолчанию – 500 миллисекунд (0,5 секунды).

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки периода ожидания Ping-операции. DHCP-сервер посылает Ping IP-адресу, чтобы определить, есть ли конфликт при использовании этого IP-адреса, прежде чем назначить IP-адрес клиенту. При отсутствии ответа по истечении определенного количества попыток IP-адрес будет присвоен клиенту и занесен в запись. При получении сервером ответа на Ping-операцию IP-адрес будет занесен в запись конфликта.

Пример

В данном примере показано, как настроить период ожидания ответа на Ping.

```
Switch# configure terminal
Switch(config)# ip dhcp ping timeout 800
Switch(config)#
```

18-17 ip dhcp pool (DHCP Server)

Данная команда используется для настройки пула DHCP-адресов DHCP-сервера и входа в режим настройки DHCP Pool Configuration Mode. Используйте форму **no** для удаления пула DHCP-адресов.

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

Параметры

NAME	Укажите имя пула. Максимально допустимое количество символов – 32.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Получив запрос от DHCP-клиента, DHCP-сервер выбирает IP-адрес из пула адресов и сообщает его клиенту. Пул адресов может содержать сеть IP-адресов или один IP-адрес. Используйте команду **network** в режиме DHCP Pool Configuration Mode, чтобы указать сеть для пула адресов. Команды **client-identifier**, **hardware-address** и **host** используются для настройки записи привязки вручную в пуле DHCP-адресов.

Пример

В данном примере показано, как создать пул DHCP-адресов. Указанное имя пула – «pool1».

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)#
```

18-18 ip dhcp use class

Данная команда используется для того, чтобы позволить DHCP-серверу использовать DHCP-классы при распределении адресов. Используйте форму **no**, чтобы отключить использование DHCP-классов.

ip dhcp use class
no ip dhcp use class

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду, чтобы включить или отключить использование классов DHCP при распределении адресов.

Пример

В данном примере показано, как отключить использование DHCP-классов.

```
Switch# configure terminal
Switch(config)# no ip dhcp use class
Switch(config)#
```

18-19 lease

Данная команда используется для настройки периода аренды IP-адреса, назначаемого из пула адресов. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

lease {*DAYS* **[***HOURS* **[***MINUTES***]] | infinite}**
no lease

Параметры

DAYS	Укажите период аренды в днях.
HOURS	(Опционально) Укажите период аренды в часах.
MINUTES	(Опционально) Укажите период аренды в минутах.
infinite	Период аренды не ограничен.

По умолчанию

Период аренды по умолчанию – 1 день.

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки периода аренды IP-адреса, присвоенного из пула адресов. Настройки родительского пула адресов не переходят на распределяемые IP-адреса автоматически.

Пример

В данном примере показано, как установить период аренды для пула адресов на 1 день. Указанное имя пула – «pool1».

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# lease 1
```

В данном примере показано, как установить период аренды для пула адресов на 1 час. Указанное имя пула – «pool1».

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# lease 0 1
```

18-20 netbios-node-type

Данная команда используется для настройки типа узла NetBIOS для DHCP-клиентов Microsoft.Используйте форму **no**, чтобы удалить настройки типа NetBIOS.

netbios-node-type *NTYPE*
no netbios-node-type

Параметры

NTYPE	Укажите тип узла NetBIOS для клиента Microsoft. Возможные типы узлов приведены ниже: **b-node** – Broadcast **p-node** – Peer-to-peer **m-node** – Mixed **h-node** – Hybrid

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки типа узла NetBIOS для DHCP-клиентов Microsoft. Рекомендуемый тип узла – H-Node (Hybrid). Тип узла определяет метод регистрации и разрешения имен, применяющийся в NetBIOS. В broadcast-системе используется тип broadcast. В системе P-Node применяются только запросы Point-to-Point на сервер имен (WINS). Система M-Node сначала начинает широковещательную рассылку, затем отправляет запрос на сервер имен. Hybrid-система сначала отправляет запрос на сервер имен, затем начинает широковещательную рассылку.

Пример

В данном примере показано, как настроить тип узла NetBIOS. Настроенный тип узла – H-Node.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# netbios-node-type h-node
Switch(config-dhcp-pool)#
```

18-21 netbios-name-server

Данная команда используется для указания WINS-серверов имен для DHCP-клиента Microsoft. Используйте форму **no** для удаления настроек указанных WINS-серверов.

netbios-name-server *IP-ADDRESS* **[***IP-ADDRESS2...IP-ADDRESS8***]**
no netbios-name-server *IP-ADDRESS* **[***IP-ADDRESS2...IP-ADDRESS8***]**

Параметры

IP-ADDRESS	Укажите IP-адрес WINS-сервера имен для DHCP-клиента.
IP-ADDRESS2...IP-ADDRESS8	Укажите несколько IP-адресов, разделяя их пробелами. Максимально допустимое количество серверов – 8.

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки IP-адресов WINS-сервера имен, доступных клиенту Microsoft. Максимально допустимое количество серверов – 8. Серверы указываются в порядке приоритетности. Если серверы имен уже настроены, то серверы, настраиваемые позже, будут добавлены в список серверов.

Пример

В данном примере показано, как настроить WINS-серверы 10.1.1.100 и 10.1.1.200 для пула адресов «pool1».

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# netbios-name-server 10.1.1.100 10.1.1.200
Switch(config-dhcp-pool)#
```

18-22 next-server

Данная команда используется для указания BOOT-сервера для DHCP-клиента. Используйте форму **no** для удаления Boot-серверов.

next-server *IP-ADDRESS*
no next-server

Параметры

IP-ADDRESS	Укажите IP-адрес Boot-сервера, чтобы обеспечить

получениеклиентом файла загрузки.

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для указания IP-адреса сервера, чтобы обеспечить загрузку файла образа клиентом. Обычно используется TFTP-сервер. Максимально допустимое количество Boot-серверов – 1.

Пример

В данном примере показано, как настроить IP-адрес Next-Server в процессе загрузки DHCP-клиента в пуле pool1. Настроенный IP-адрес – 10.1.1.1.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# next-server 10.1.1.1
```

18-23 network

Данная команда используется для того, чтобы настроить подсеть для пула DHCP-адресов. Используйте форму **no** для удаления подсети.

network {*NETWORK-ADDRESS MASK* **|** *NETWORK-ADDRESS***/***PREFIX-LENGTH***}**
no network

Параметры

NETWORK-ADDRESS	Укажите адрес подсети для пула адресов.
MASK	Укажите биты, определяющие сетевую маску.
PREFIX-LENGTH	Укажите длину префикса сети (это альтернативный способ указать сетевую маску).

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется в режиме DHCP Pool Configuration Mode, чтобы настроить подсеть для пула адресов. Невозможно сконфигурировать запись привязки вручную для того пула адресов, в котором указана подсеть.

Получая запрос от клиента, DHCP-сервер выбирает пул адресов или подсеть в пуле адресов на основе нижеуказанных правил распределения адресов. После присвоения узлу IP-адреса создается запись привязки.

- Если клиент не подключен к DHCP-серверу напрямую, сообщение Discover передается при помощи Relay Agent. Сервер выберет пул адресов с настроенной подсетью, содержащей GIADDR пакета, а затем присвоит адрес.
- Если клиент подключен к серверу напрямую, то сервер будет искать пулы, на которых настроена подсеть, которая соответствует подсети принимающего интерфейса.

Если адрес присвоен из указанной подсети, то сетевая маска, связанная с подсетью, будет использована в качестве сетевой маски пользователя. В качестве сети, настраиваемой для пула DHCP-адресов, может выступать сеть или подсеть. Настраиваемый пул DHCP-адресов организован в виде дерева: пул адресов, содержащий сеть, можно сравнить с корнем, пулы адресов, содержащие подсети – с ветвями, а пулы адресов, содержащие записи привязки вручную – с листьями. Дочерний пул адресов будет использовать все настройки родительского пула, кроме настроек аренды.

Пример

В данном примере показано, как настроить подсеть 10.1.0.0/16 для пула DHCP-адресов pool1.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# network 10.1.0.0/16
Switch(config-dhcp-pool)# default-router 10.1.1.1
Switch(config-dhcp-pool)#
```

18-24 option hex (DHCP Server)

Эта команда используется для указания шаблона соответствия опций DHCP для класса DHCP. Используйте форму **no** этой команды для удаления указанного шаблона соответствия для класса DHCP.

option *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**
no option *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**

Параметры

CODE	Укажите номер DHCP-опции.
PATTERN	Укажите шестнадцатеричный шаблон указаннойDHCP-опции.
*	Укажите биты опции, которые не будут проверяться на соответствие. При отсутствии отметки со знаком * длина шаблона опции должна быть равна битовой длине опции.
MASK	Укажите шестнадцатиричную битовую маску для шаблона. Указанные биты в маске будут проверены. Если маска не

	указана, будут проверены все биты, указанные в шаблоне. Будет проверен бит со значением 1. Формат ввода должен быть идентичен шаблону.

По умолчанию

Нет

Режим ввода команды

DHCP Class Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда **ip dhcp class**, наряду с командой **option hex**, может применяться для определения DHCP-класса. Классы в пуле распределяются в том порядке, в котором они настроены в пулеадресов.

Команда **option hex** применяется для указания номера DHCP-опции и сопоставления ему DHCP-класса. Для одного DHCP-класса можно указать несколько шаблонов опции. Если пакет соответствует какому-либо из указанных шаблонов, он будет причислен к DHCP-классу и передан вуказанное место назначения.

Ниже перечислены некоторые часто используемые коды опций:

- Option 60 (Vendor Class Identifier).
- Option 61 (Client Identifier).
- Option 77 (User Class).
- Option 82 (Relay Agent Information Option).
- Option 124 (Vendor-Identifying Vendor Class).
- Option 125 (Vendor-Identifying Vendor-Specific Information).

Пример

В данном примере показано, как настроить DHCP-класс Service-A и установить соответствие с ним шаблонов 0x112233 и 0x102030 Option 60 DHCP. Другой класс Service-B соответствует шаблонам 0x5566* и 0x5060* Option 60 DHCP.

```
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 class Service-B
Switch(config-dhcp-class)# option 60 hex 5566 *
Switch(config-dhcp-class)# option 60 hex 5060 *
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp class Service-B
Switch(config-dhcp-class)#
```

18-25 service dhcp

Данная команда используется для включения DHCP-сервера и Relay Service. Для отключения данной команды используйте форму **no**.

service dhcp
no service dhcp

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для включения службы сервера DHCP на коммутаторе.

Пример

В этом примере показано, как отключить службу сервера DHCP.

```
Switch# configure terminal
Switch(config)# no service dhcp
Switch(config)#
```

18-26 show ip dhcp binding

Данная команда используется для отображения записей привязки адресов DHCP-сервера.

show ip dhcp binding [*IP-ADDRESS***]**

Параметры

IP-ADDRESS	(Опционально) Укажите, чтобы отобразить запись привязки. Если IP-адрес не указан, отображаются все записи привязки или записи привязки указанного пула.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Будет отображен IP-адрес, аппаратный адрес, сроки начала и истечения периода аренды записи.

Пример

В данном примере показано, как отобразить статус привязки всех связанных IP-адресов.

```
Switch#show ip dhcp binding

 IP address          Client-ID/     Lease expiration    Type
                   Hardware address
 --------------- ----------------- -------------------- ---------
 10.0.0.1        01002211223344    Feb 25 2017 08:18 AM Automatic

Switch#
```

В данном примере показано, как отобразить статус привязки IP-адреса 10.1.1.1 в пуле DHCP адресов.

```
Switch#show ip dhcp binding

 IP address          Client-ID/     Lease expiration    Type
                   Hardware address
 --------------- ----------------- -------------------- ---------
 10.1.1.1        01002211223344    Feb 25 2017 08:21 AM Automatic

Switch#
```

18-27 show ip dhcp conflict

Данная команда используется для отображения адресных конфликтов при попытках DHCP-сервера присвоить IP-адрес клиенту.

show ip dhcp conflict [*IP-ADDRESS*]

Параметры

IP-ADDRESS	(Опционально) Укажите, чтобы отобразить запись конфликта. Если IP-адрес не указан, отображаются все записи конфликта или записи конфликта указанного пула.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

DHCP-сервер обнаруживает конфликт IP-адресов при помощи Ping-операции. При обнаружении адресного конфликта данный IP-адрес будет удален из пула адресов и отмечен в качестве конфликтного. Этот адрес не может быть присвоен клиенту, пока администратор не устранит адресный конфликт.

Пример

В данном примере показано, как отобразить конфликтный статус IP-адреса 10.1.1.1.

```
Switch# show ip dhcp conflict 10.1.1.1

 IP address      Detected Method Detection time
 --------------- --------------- --------------------
 10.1.1.1        Ping            Oct 23 2013 09:12 AM

Switch#
```

В данном примере показано, как отобразить конфликтный статус всех IP-адресов DHCP-пула.

```
Switch#show ip dhcp conflict

 IP address      Detected Method Detection time
 --------------- --------------- --------------------
 10.1.1.1        Ping            Oct 23 2013 09:12 AM

Switch#
```

18-28 show ip dhcp pool

Данная команда используется для отображения информации о DHCP-пуле.

show ip dhcp pool [*NAME***]**

Параметры

NAME	(Опционально) Укажите, чтобы отобразить информацию о DHCP-пуле. Если значение не задано, будет отображена информация обо всех DHCP-пулах.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы просмотреть параметры настроек пула. Если значение не задано, будут отображены параметры конфигурации всех пулов.

Пример

В данном примере показано, как отобразить информацию о настройках DHCP-пула «pool1».

```
Switch#show ip dhcp pool pool1

 Pool name: pool1
   Network: 10.0.0.0/8
   Boot file:
   Default router:
   DNS server:
   NetBIOS server:
   Domain name:
   Lease: 1 days 0 hours 0 minutes
   NetBIOS node type:
   Next server: 0.0.0.0
   Remaining unallocated address number: 1023
   Number of leased addresses: 1


Switch#
```

18-29 show ip dhcp server

Данная команда используется для отображения текущего статуса DHCP-сервера.

show ip dhcp server

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить статус DHCP-сервера и пул адресов, настроенный пользователем.

Пример

В данном примере показано, как отобразить статус DHCP-сервера.

```
Switch# show ip dhcp server

DHCP Service: Disable
Ping packets number: 3
Ping timeout: 500 ms
Excluded Addresses
10.1.1.1-10.1.1.255

List of DHCP server configured address pool
pool1               pool2               pool3               pool4
pool5               pool6               pool7               pool8
pool9               pool10              pool11              pool12

Switch#
```

18-30 show ip dhcp server statistics

Данная команда используется для отображения статистики DHCP-сервера.

show ip dhcp server statistics

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить счетчики DHCP. Все счетчики суммируются.

Пример

В данном примере показано, как отобразить статистику DHCP-сервера.

```
Switch# show ip dhcp server statistics

Address pools               3
Automatic bindings          100
Manual binding              2
Malformed messages          0
Renew messages              0

Message             Received
BOOTREQUEST                 12
DHCPDISCOVER                200
DHCPREQUEST                 178
DHCPDECLINE                 0
DHCPRELEASE                 0
DHCPINFORM                  0

Message                 Sent
BOOTREPLY               12
DHCPOFFER               190
DHCPACK                 172
DHCPNAK                  6

Switch#
```

Отображаемые параметры

Address pools	Количество пулов, настроенных в базе данных DHCP.
Malformed messages	Количество поврежденных сообщений, полученных DHCP сервером.
Renew messages	Количество Renew-сообщений для времени аренды DHCP. Счетчик увеличивается, когда поступает новое Renew-сообщение о продлении аренды.
Message	Тип DHCP-сообщения.
Received	Количество DHCP-сообщений, полученных DHCP-сервером.
Sent	Количество DHCP-сообщений, отправленных DHCP-сервером.

19. Команды DHCP Snooping

19-1 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Функция DHCP Snooping отслеживает пакеты DHCP, поступающие на недоверенный интерфейс во VLAN, на котором включена данная функция. С помощью данной функции DHCP-пакеты, приходящие с недоверенного интерфейса, могут получить статус проверенных и будет создана таблица привязки DHCP для DHCP Snooping во 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)#
```

19-2 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Функция DHCP Snooping проверяет пакеты DHCP, когда они поступают на порт во VLAN, на котором включена функция DHCP Snooping. По умолчанию при проверке будут отброшены пакеты, если их адрес шлюза не равен 0 или присутствует Option 82.

Используйте данную команду, чтобы разрешить 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)#
```

19-3 ip dhcp snooping database

Данная команда используется для настройки хранения записей привязки DHCP Snooping в локальной файловой системе (флеш-карте) или на удаленном узле. При использовании формы **no** команда отключит хранение или вернется к настройкам по умолчанию.

ip dhcp snooping database {*URL* **/write-delay** *SECONDS***}**
no ip dhcp snooping database [write-delay]

Параметры

URL	Укажите URL в каком-либо из представленных форматов: • 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 доступных 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для хранения записей привязки DHCP в локальной Flash-памяти или на удаленном узле. Используйте следующие методы для хранения записей привязки DHCP:

- **tftp:** хранение записей на удаленном узле через TFTP.

Используйте данную команду, чтобы сохранить таблицу привязки DHCP Snooping в коммутаторе стека. Таблица не будет сохранена в отдельных коммутаторах стека.

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 файловой системы.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping database tftp: //10.0.0.2/store/dhcp-snp-bind
Switch(config)#
```

19-4 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

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#
```

19-5 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

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#
```

19-6 renew ip dhcp snooping database

Данная команда используется для обновления таблицы привязки DHCP.

renew ip dhcp snooping database *URL*

Параметры

URL	Укажите URL места, из которых нужно загружать таблицу привязки для обновления. URL может быть в одном из следующих форматов: • tftp://location/filename

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Использование этой команды заставит систему загрузить базу данных записей привязки из URL и добавить записи в таблицу записей 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#
```

19-7 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 (физический порт или port-channel), 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная 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 в VLAN 2 и порту 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 ethernet 1/0/10
expiry 100
Switch#
```

19-8 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет настроить физический порт и port-channel интерфейс.

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 или DHCPLEASEQUERY) 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 Snopping, и информация об интерфейсе в таблицепривязки не соответствует интерфейсу, на котором было получено сообщение.

В дополнение к процессу проверки DHCP Snooping также создает запись привязки на основе IP- адреса, назначенного клиенту сервером в таблице привязки DHCP Snooping. 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 этом примере показано, как включить доверие DHCP snooping для порта 3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)#
```

19-9 ip dhcp snooping limit entries

Данная команда используется для настройки количества записей привязки DHCP Snooping, которыеможет изучить интерфейс. При использовании формы **no** команда сбросит значение лимита записейDHCP.

ip dhcp snooping limit entries {*NUMBER***}**
no ip dhcp snooping limit entries

Параметры

NUMBER	Укажите лимит количества привязок DHCP Snooping на порт. Диапазон допустимых значений: от 0 до 1024.

По умолчанию

По умолчанию этот параметр имеет значение **no-limit**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет настроить физический порт и интерфейс port-channel. Команда действует только на недоверенных интерфейсах. Система перестанет изучать привязки, связанные с портом, если превышено максимальное значение.

Пример

В этом примере показано, как настроить ограничение на количество записей привязки, разрешенных на порту 1 до 100.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ip dhcp snooping limit entries 100
Switch(config-if)#
```

19-10 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 лимита 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. Диапазон допустимых значений: от 1 до 300.

По умолчанию

По умолчанию ограничений нет.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

При превышении лимита количества DHCP-пакетов за секунду порт будет отключен из-за ошибки.

Пример

В этом примере показано, как настроить количество сообщений DHCP, которые коммутатор может принимать в секунду на порту 3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)#
```

19-11 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

Уровень команды по умолчанию

Уровень 12

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)#
```

19-12 ip dhcp snooping verify mac-address

Данная команда используется для включения проверки совпадения MAC-адреса источника DHCP-пакета 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Функция DHCP Snooping проверяет DHCP пакеты, присылаемые на порт во VLAN, на которой включена функция DHCP Snooping. По умолчанию DHCP Snooping проверяет, совпадает ли MAC- адрес источника в заголовке Ethernet с аппаратным адресом DHCP-клиента, чтобы пройти проверку.

Пример

В данном примере показано, как включить проверку на соответствие MAC-адреса источника DHCP- пакета аппаратному адресу клиента.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping verify mac-address
Switch(config)#
```

19-13 ip dhcp snooping vlan

Данная команда используется для включения DHCP Snooping во VLAN или группе VLAN. При использовании формы **no** команда отключит DHCP Snooping во VLAN или группе VLAN.

ip dhcp snooping vlan *VLAN-ID* **[, | -]**
no ip dhcp snooping vlan *VLAN-ID* **[, | -]**

Параметры

VLAN-ID	Укажите VLAN, в которой необходимо включить или отключить функцию DHCP Snooping.
,	(Опционально) Выделение серии VLAN или разделение группы VLAN отпредыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Выделение диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию функция DHCP Snooping отключена во всех VLAN.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для глобального включения DHCP Snooping, используйте команду **ip dhcp snooping vlan** для включения DHCP Snooping для VLAN. Функция DHCP Snooping отслеживает пакеты DHCP, приходящие на недоверенный интерфейс во VLAN, на которой включена функция DHCP snooping. С помощью данной функции DHCP-пакеты, приходящие с недоверенного интерфейса, могут получить статус проверенных, а таблица привязки DHCP будет создана для DHCP Snooping во VLAN. Таблица привязки предоставляет информацию о привязке IP и MAC, которая позже может использоваться IP Source Guard и Dynamic ARP Inspection.

Пример

В данном примере показано, как включить DHCP Snooping во VLAN 10.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping vlan 10
Switch(config)#
```

В данном примере показано, как включить DHCP Snooping в нескольких VLAN.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping vlan 10,15-18
Switch(config)#
```

19-14 show ip dhcp snooping

Данная команда используется для отображения настроек DHCP Snooping.

show ip dhcp snooping

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения параметров настроек DHCP Snooping.

Пример

В данном примере показано, как включить отображение параметров настроек DHCP Snooping.

```
Switch# show ip dhcp snooping

DHCP Snooping is enabled
DHCP Snooping is enabled on VLANs:
          10, 15-18
Verification of MAC address is disabled
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        50           no_limit
eth1/0/3       yes       no_limit     no_limit

Switch#
```

19-15 show ip dhcp snooping binding

Данная команда используется для отображения 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 *INTERFACE-ID*	(Опционально) Укажите, если необходимо отображать привязки на основе ID порта (port ID).
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Выделение диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения привязки DHCP Snooping.

Пример

В данном примере показано, как настроить отображение 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 настроить отображение привязки DHCP Snooping по IP 10.1.1.1.

```
Switch# show ip dhcp snooping binding 10.1.1.1

MAC Address       IP Address      Lease (seconds)   Type           VLAN   Interface
----------------- --------------- ----------------  -------------- ------ ----------
00-01-02-03-04-05 10.1.1.1        1500              dhcp-snooping  100    eth1/0/5

Total Entries: 1

Switch#
```

В данном примере показано, как настроить отображение привязки DHCP Snooping по IP 10.1.1.11 и MAC 00-01-02-00-00-05.

```
Switch# show ip dhcp snooping binding 10.1.1.11 00-01-02-00-00-05

MAC Address       IP Address      Lease(seconds) Type           VLAN Interface
----------------- --------------- -------------- -------------- ---- --------------
00-01-02-00-00-05 10.1.1.11       1495           dhcp-snooping 100  eth1/0/5

Total Entries: 1

Switch#
```

В данном примере показано, как настроить отображение привязки DHCP Snooping по IP 10.1.1.1 и MAC 00-01-02-03-04-05 во VLAN 100.

```
Switch# show ip dhcp snooping binding 10.1.1.11 00-01-02-00-00-05 vlan 100

MAC Address       IP Address      Lease(seconds) Type           VLAN Interface
----------------- --------------- -------------- -------------- ---- --------------
00-01-02-03-04-05 10.1.1.1        1500           dhcp-snooping 100  eth1/0/5

Total Entries: 1

Switch#
```

В данном примере показано, как настроить отображение привязки DHCP Snooping во 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 данном примере показано, как настроить отображение привязки DHCP Snooping на интерфейсе Ethernet 1/0/5.

```
Switch# show ip dhcp snooping binding interface ethernet 1/0/5

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-адрес	Аппаратный MAC-адрес клиента.
IP-адрес	IP-адрес клиента, назначенный DHCP-сервером.
Время аренды (lease) (в секундах)	Время аренды IP-адреса.
Тип	Тип привязки, настроенный через интерфейс командной строки или изученный динамически.
VLAN	VLAN ID.
Interface	Интерфейс, подключающийся к узлу DHCP-клиента.

19-16 show ip dhcp snooping database

Данная команда используется для отображения статистики таблицы привязки DHCP Snooping.

show ip dhcp snooping database

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения статистики таблицы привязки DHCP Snooping.

Пример

В данном примере показано, как включить отображение статистики таблицы привязки 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 привязки DHCP Snooping.
Expired leases	Количество записей с истекшим сроком аренды в таблице привязки DHCP Snooping.
Invalid interfaces	Количество интерфейсов, получивших сообщение DHCP, но DHCP Snooping для которых не выполняется.
Pase failures	Количество недопустимых пакетов DHCP.
Checksum errors	Количество подсчитанных значений checksum, не равное сохраненному значению checksum.
Unsupported vlans	Количество записей, для которых VLAN отключена.

19-17 based-on hardware-address

Эта команда используется для добавления записи профиля экрана сервера DHCP. Используйте форму **no** этой команды для удаления указанной записи.

based-on hardware-address *CLIENT-HARDWARE-ADDRESS*
no based-on hardware-address *CLIENT-HARDWARE-ADDRESS*

Параметры

CLIENT-HARDWARE-ADDRESS	(Опционально) Укажите MAC-адрес клиента.

По умолчанию

Нет

Режим ввода команды

DHCP Server Screen Configure Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если запись привязки определена с MAC-адресом клиента, то сообщение сервера с указанным IP-адресом сервера и адресом клиента в полезной нагрузке будет разрешено. Эти записи привязки ограничивают, что только определенным серверам разрешено предлагать адреса для обслуживания определенных клиентов.

Если запись привязки определена без MAC-адреса клиента, то будет разрешено сообщение сервера с указанным IP-адресом сервера в полезной нагрузке. Эти записи привязки ограничивают возможность предоставления услуг сервера DHCP только определенным серверам.

Пример

В этом примере показано, как настроить профиль экрана DHCP-сервера с именем "campus-profile", который содержит 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)#
```

19-18 clear ip dhcp snooping server-screen log

Эта команда используется для очистки буфера журнала экрана сервера.

clear ip dhcp snooping server-screen log

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для очистки буфера журнала экрана сервера. Буфер журнала экрана сервера DHCP отслеживает информацию о пакетах, которые не прошли проверку. Первый пакет, нарушивший проверку, будет отправлен в модуль журнала и записан в буфер журнала экрана сервера. Последующие пакеты, относящиеся к той же сессии, не будут отправляться в модуль регистрации, пока не будет очищена запись в буфере регистрации.

Пример

В этом примере показано, как очистить журнал экрана сервера.

```
Switch# clear ip dhcp snooping server-screen log
Switch#
```

19-19 dhcp-server-screen profile

Эта команда используется для определения профиля экрана сервера и входа в режим настройки экрана сервера DHCP. Используйте форму **no** этой команды для удаления указанного профиля экрана сервера.

dhcp-server-screen profile *PROFILE-NAME*
no dhcp-server-screen profile *PROFILE-NAME*

Параметры

PROFILE-NAME	Указывает имя профиля, содержащее не более 32 символов.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для входа в режим настройки экрана сервера DHCP для определения профиля экрана сервера. Профиль можно использовать для определения записи экрана сервера DHCP.

Пример

В данном примере показано, как войти в режим настройки экрана DHCP-сервера для определения профиля " campus".

```
Switch# configure terminal
Switch(config)# service dhcp
switch(config)# dhcp-server-screen profile campus
switch(config-dhcp-server-screen)#
```

19-20 ip dhcp snooping server-screen

Эта команда используется для включения проверки DHCP-сервера. Используйте форму **no** этой команды, чтобы отключить ее.

ip dhcp snooping server-screen [*SERVER-IP-ADDRESS* **[profile** *PROFILE-NAME***]]**
no ip dhcp snooping server-screen [*SERVER-IP-ADDRESS***]**

Параметры

PROFILE-NAME	(Опционально) Указывает профиль со списком MAC-адресов клиентов для DHCP-сервера.
SERVER-IP-ADDRESS	(Опционально) Укажите IP-адрес доверительного DHCP-сервера.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Функция отсеивания DHCP-сервера используется для фильтрации пакетов DHCP-сервера на определенном интерфейсе и получения доверительных пакетов от определенного источника. Эта функция может сделать защищенную сеть пригодной для использования, когда вредоносный узел отправляет пакеты DHCP-сервера.

Если IP-адрес сервера не указан, это включит или отключит экран DHCP-сервера на интерфейсе. По умолчанию экран DHCP-сервера отключен на всех интерфейсах. Если экран DHCP-сервера включен, на определенном интерфейсе он будет фильтровать все пакеты DHCP-сервера с интерфейса и пересылать только пакеты доверенного сервера.

Если запись экрана сервера определена с профилем, который содержит MAC-адрес клиента, то пересылается сообщение сервера с IP-адресом сервера и адресами клиентов, содержащимися в профиле.

Если запись определена без MAC-адреса клиента, то будет перенаправлено сообщение сервера с указанным IP-адресом сервера. Каждый сервер может иметь только одну соответствующую запись в таблице.

Если запись определена с профилем, но такой записи не существует, то сообщения с IP-адресом сервера, указанным этой записью, не пересылаются.

Пример

В этом примере показано, как настроить профиль экрана сервера DHCP с именем "campus-profile" и связать его с записью экрана сервера DHCP на порту 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)#
```

19-21 ip dhcp snooping server-screen log-buffer

Эта команда используется для настройки параметра буфера журнала экрана DHCP-сервера. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

ip dhcp snooping server-screen log-buffer entries *NUMBER*
no ip dhcp snooping server-screen log-buffer entries

Параметры

NUMBER	Указывает номер записи в буфере. Максимальное число - 1024.

По умолчанию

По умолчанию это значение равно 32.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для настройки максимального количества записей в буфере журнала. Буфер журнала экрана сервера DHCP сохраняет информацию о пакетах, которые не прошли проверку. Первый пакет, нарушивший проверку, будет отправлен в модуль журнала и записан в буфер журнала экрана сервера.

Последующие пакеты, принадлежащие той же сессии, не будут отправляться в модуль журнала, пока не будет очищена запись в буфере журнала.

Если буфер журнала заполнен, но происходит больше событий нарушения, пакеты будут отброшены, но событие не будет отправлено в модуль syslog. Если пользователь укажет размер буфера меньше, чем номер текущей записи, то буфер журнала будет автоматически очищен.

Пример

В этом примере показано, как изменить максимальное число буферов на 64.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping server-screen log-buffer entries 64
Switch(config)#
```

19-22 show ip dhcp server-screen log

Эта команда используется для отображения буфера журнала экрана сервера.

show ip dhcp server-screen log

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду для отображения содержимого буфера журнала экранов DHCP-сервера. В буфере хранится информация о сообщениях сервера, нарушающих экранирование. Отслеживается количество повторений одного и того же нарушения и последнее время появления.

Пример

В этом примере показано, как отобразить буфер журнала экрана сервера DHCP.

```
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#
```

19-23 snmp-server enable traps dhcp-server-screen

Эта команда используется для включения отправки SNMP-уведомлений для атаки forge DHCP Server. Для отключения отправки SNMP-уведомлений используйте форму **no** этой команды.

snmp-server enable traps dhcp-server-screen
no snmp-server enable traps dhcp-server-screen

Параметры

Нет

По умолчанию

По умолчанию эта опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если включен экран сервера DHCP и коммутатор получает поддельный пакет сервера DHCP, коммутатор будет регистрировать событие, если получен какой-либо атакующий пакет. Вы можете использовать эту команду для включения или отключения отправки SNMP-уведомлений для таких событий.

Пример

В этом примере показано, как включить отправку ловушек для проверки DHCP-сервера.

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

20. Команды DHCPv6 Client

20-1 clear ipv6 dhcp client

Данная команда используется для перезапуска DHCPv6 Client на интерфейсе.

clear ipv6 dhcp client *INTERFACE-ID*

Параметры

INTERFACE-ID	Укажите интерфейс VLAN, для которого необходимо перезапустить DHCPv6 Client.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для перезапуска IPv6 DHCP Client на указанном интерфейсе.

Пример

В данном примере показано, как перезапустить DHCPv6 Client для интерфейса VLAN 1.

```
Switch# clear ipv6 dhcp client vlan 1
Switch#
```

20-2 show ipv6 dhcp

Данная команда используется для отображения настроек DHCPv6 на интерфейсе.

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

Параметры

INTERFACE-ID	Укажите интерфейс VLAN, для которого необходимо отобразить настройки DHCPv6.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить DHCPv6 DUID устройства, или используйте команду **show ipv6 dhcp interface**, чтобы отобразить настройки DHCPv6 для интерфейсов. 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 0001000111A8040D001FC6D1D47B.

Switch#
```

В данном примере показано, как отобразить настройки DHCPv6 для интерфейса VLAN 1, если на VLAN 1 отключена функция DHCPv6.

```
Switch# show ipv6 dhcp interface vlan 1

vlan 1 is not in DHCPv6 mode.

Switch#
```

В данном примере показано, как отобразить настройки DHCPv6 для всех VLAN. Отображаются только те VLAN, на которых включена функция DHCPv6.

```
Switch# show ipv6 dhcp interface

vlan 1 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#
```

21. Команды DHCPv6 Guard

21-1 ipv6 dhcp guard policy

Данная команда используется для создания или изменения политики DHCPv6 Guard Policy. Команда позволяет войти в режим DHCPv6 Guard Configuration Mode. При использовании формы **no** данная команда удалит политику DHCPv6 Guard.

ipv6 dhcp guard policy *POLICY-NAME*
no ipv6 dhcp guard policy

Параметры

POLICY-NAME	Укажите имя политики DHCPv6 Guard.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для создания или изменения политики DHCPv6 Guard Policy. 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** дляприменения 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)#
```

21-2 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

Уровень команды по умолчанию

Уровень 12

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 dhcpguard1
Switch(config-dhcp-guard)# device-role server
Switch(config-dhcp-guard)#
```

21-3 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для фильтрации DHCPv6-сообщений сервера на основе IP-адресаисточника. Если не настроена команда **match ipv6 access-list,** все сообщения сервера будут игнорироваться. 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)#
```

21-4 ipv6 dhcp guard attach-policy

Данная команда используется для применения политики DHCPv6 Guard Policy на определенном интерфейсе. При использовании формы **no** данная команда удалит привязку.

ipv6 dhcp guard attach-policy [*POLICY-NAME*]
no ipv6 dhcp guard attach-policy

Параметры

POLICY-NAME	Укажите список доступа IPv6, с которым необходимо сверяться.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 этом примере показано применение политики защиты DHCPv6 "pol1" к порту 3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ipv6 dhcp guard attach-policy pol1
Switch(config-if)#
```

21-5 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Если указано имя политики, то отображаться будет информация только для нее. Если имя политики не указано, отображаться будет информация для всех политик.

Пример

В данном примере показано, как включить отображение информации 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. Ролью может быть клиент или сервер.
Target	Название интерфейса.
Source Address Match Access List	Список доступа IPv6 определенной политики.

22. Команды DHCPv6 Relay

22-1 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. Используйте форму **no**, чтобы удалить Relay Destination.

ipv6 dhcp relay destination *IPV6-ADDRESS* [*INTERFACE-ID*]
no ipv6 dhcp relay destination *IPV6-ADDRESS*

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Чтобы включить на интерфейсе функцию DHCPv6 Relay, настройте адрес Relay Destination при помощи команды **ipv6 dhcp relay destination**. Чтобы удалить адрес Relay, используйте команду **noipv6 dhcp relay destination**. При удалении всех адресов Relay функция Relay 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 этом примере показано, как настроить адрес назначения реле на VLAN 1 и VLAN 2.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 vlan 1
Switch(config-if)# ipv6 dhcp relay destination FE80::22:33 vlan 2
Switch(config-if)#
```

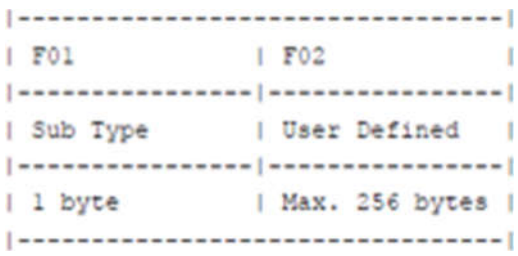
22-2 ipv6 dhcp relay remote-id format

Данная команда используется для настройки sub-опции Remote ID. Используйте форму **no**, чтобывернуться к настройкам по умолчанию.

ipv6 dhcp relay remote-id format {default | cid-with-user-define | user-define}
no ipv6 dhcp relay remote-id format

Параметры

default	Укажите, чтобы использовать системный MAC-адрес коммутатора в качестве Remote ID. 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.** *Tun sub-опции:* число 1 свидетельствует о том, что тип данного ID – Remote ID. **F02.** *VLAN ID:* входящий VLAN ID в пакете DHCP Client. **F03.** *ID модуля:* ID модуля для автономных коммутаторов – 0.ID модуля для стекированных коммутаторов – Unit ID. **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	Укажите, чтобы использовать CID со строкой, заданной пользователем, в качестве Remote ID. Формат Remote ID представлен ниже: | F01 | F02 | F03 | F04 | F05 | | Sub Type | VLAN ID | Module ID | Port ID | User Defined | | 1 byte | 2 bytes | 1 byte | 1 byte | Max. 256 bytes | **F01.** *Tun sub-опции:* число 2 свидетельствует о том, что тип

	данного ID – Remote ID. **F02.** *VLAN ID:* входящий VLAN ID в пакете DHCP Client. **F03.** *ID модуля:* ID модуля для автономных коммутаторов – 0. ID модуля для стекированных коммутаторов – Unit ID. **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 relayremote-id udf**. По умолчанию данное поле не заполнено.
user-define	Укажите, чтобы задать Remote ID самостоятельно. Формат Remote ID представлен ниже:  **F01.** *Tun sub-опции:* число 3 свидетельствует о том, что тип данного ID – Remote ID. **F02.** *Задать самостоятельно:* заданная пользователем строка, настраиваемая при помощи команды **ipv6 dhcp relayremote-id udf**.

По умолчанию

Формат DHCPv6 Relay Remote ID по умолчанию – **default**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

22-3 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. Используйте форму **no**, чтобы отключить данную функцию.

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

Уровень команды по умолчанию

Уровень 12

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)#
```

22-4 ipv6 dhcp relay remote-id policy

Данная команда используется для настройки политики перенаправления Option 37 для DHCPv6 Relay Agent. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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 напрямую ретранслировать пакет запроса DHCPv6, в котором уже есть Relay Agent Remote ID Option, на сервер DHCPv6 в неизменном виде.

По умолчанию

Параметр по умолчанию – **keep**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 уже присутствует RelayAgent Remote ID Option, будет отброшен. При выборе политики **keep** коммутатор не будет проверять, присутствует ли в полученном пакете Relay Agent Remote ID Option.

Пример

В данном примере показано, как настроить политику DHCPv6 Relay Agent Remote ID Option так, чтобы пакет был отброшен при наличии в нем Relay Agent Remote ID Option.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id policy drop
Switch(config)#
```

22-5 ipv6 dhcp relay remote-id udf

Используйте данную команду, чтобы настроить User Define Field (UDF) для Remote ID. Используйте форму **no**, чтобы удалить запись UDF.

ipv6 dhcp relay remote-id udf {ascii *STRING* **| hex** *HEX-STRING***}**
no ipv6 dhcp relay remote-id udf

Параметры

ascii *STRING*	Укажите строку ASCII для UDF Remote ID. Максимально допустимое количество символов – 128.
hex *HEX-STRING*	Укажите шестнадцатеричную строку для UDF Remote ID. Максимально допустимое количество знаков – 256.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 данном примере показано, как настроить UDF (шестнадцатеричная строка) «010c08».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id udf hex 010c08
Switch(config)#
```

22-6 show ipv6 dhcp

Данная команда используется для отображения настроек DHCPv6 на интерфейсе.

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

Параметры

INTERFACE-ID	(Опционально) Укажите ID интерфейса VLAN, который необходимо отобразить.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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#
```

22-7 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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#
```

23. Команды DHCPv6 Server

23-1 address prefix

Данная команда используется для указания префикса адреса, который будет присвоен клиенту. Используйте форму **no**, чтобы удалить префикс адреса.

address prefix *IPV6-PREFIX*/*PREFIX-LENGTH* **[lifetime** *VALID-LIFETIME PREFERRED-LIFETIME***]**
no address prefix

Параметры

IPV6-PREFIX	Укажите префикс IPv6-адреса, который необходимо присвоить клиенту.
PREFIX-LENGTH	Укажите длину префикса IPv6-адреса.
lifetime *VALID-LIFETIME*	(Опционально) Указывает действительное время жизни префикса адреса в секундах. Значение действительного времени жизни должно быть больше, чем предпочтительное время жизни. Это значение должно быть от 60 до 4294967295 или бесконечным. Если время жизни не указано, значение времени жизни по умолчанию равно 2592000 секунд (30 дней).
PREFERRED-LIFETIME	(Опционально) Указывает предпочтительное время жизни префикса адреса в секундах. Это значение должно быть от 60 до 4294967295 или бесконечным. Если значение времени жизни не указано, время жизни по умолчанию равно 604800 секунд (7 дней).

По умолчанию

Нет

Режим ввода команды

DHCPv6 Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить префикс адреса в пуле IPv6 DHCP. В DHCPv6-пуле можно настроить только один префикс адреса. Последующая команда будет замещать предыдущую.

Получив запрос от клиента, сервер проверит пул IPv6 DHCP, ассоциированный с получающим интерфейсом. Если статические записи привязки адреса настроены так, чтобы присваивать адрес запрашивающему клиенту, будет присвоен адрес статической привязки. Иначе сервер присвоит адрес из префикса адреса, указанного для пула IPv6 DHCP.

Пример

В данном примере показано, как настроить префикс адреса 2001:0DB8::0/64 для пула IPv6 DHCP «pool1».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# address prefix 2001:0DB8::0/64 lifetime 200 100
Switch(config-dhcp)#
```

23-2 address-assignment

Данная команда используется для указания адреса, который необходимо присвоить обозначенному клиенту. Используйте форму **no**, чтобы удалить адрес статической привязки.

address-assignment *IPV6-ADDRESS/PREFIX-LENGTH CLIENT-DUID* **[iaid** *IAID***] [lifetime** *VALID-LIFETIME PREFERRED-LIFETIME***]**
no address-assignment *IPV6-ADDRESS/PREFIX-LENGTH*

Параметры

IPV6-PREFIX	Укажите IPv6-адрес, который необходимо присвоить обозначенному клиенту.
PREFIX-LENGTH CLIENT-DUID	Укажите длину IPv6-префикса. Укажите DHCP Unique Identifier (DUID) клиента, которому необходимо присвоить адрес.
iaid *IAID*	(Опционально) Указывает идентификатор ассоциации идентификации (IAID). IAID здесь уникально идентифицирует набор не временных адресов (IANA), назначенных на клиенте.
lifetime *VALID-LIFETIME*	(Опционально) Указывает срок действия адреса в секундах. Действительное время жизни должно быть больше, чем предпочтительное время жизни. Это значение должно быть от 60 до 4294967295 или бесконечным. Если время жизни не указано, время жизни по умолчанию составляет 2592000 секунд (30 дней).
PREFERRED-LIFETIME	(Опционально) Указывает предпочтительное время жизни адреса в секундах. Это значение должно быть от 60 до 4294967295 или бесконечным. Если время жизни не указано, предпочтительное время жизни по умолчанию составляет 604800 секунд (7 дней).

По умолчанию

Нет

Режим ввода команды

DHCPv6 Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить статическую запись привязки адреса так, чтобы она указывала адрес, который необходимо присвоить обозначенному клиенту.

Получив запрос от клиента, сервер проверит пул IPv6 DHCP, ассоциированный с полученным интерфейсом. Если сообщение Request содержит опцию IANA и имеются свободные статические записи, настроенные с IAID и соответствующие DUID и IAID сообщения, соответствующая запись будет присвоена. Если соответствующая запись отсутствует, но имеются свободные статические записи без указанных IAID, которые соответствуют DUID сообщения, на соответствующую запись будет отправлен ответ.

При отсутствии соответствующих записей клиенту будет присвоен адрес из префикса адреса, указанного в пуле IPv6 DHCP.

Пример

В данном примере показано, как настроить статическую запись привязки адреса в пуле IPv6 DHCP «pool1» и ассоциировать пул IPv6 DHCP с VLAN 100.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(dhcpv6-config)# address-assignment 2001:0DB8::1:2 000300010506BBCCDDEE
Switch(dhcpv6-config)# exit
Switch(config)# interface vlan 100
Switch(dhcpv6-config)# ipv6 dhcp server pool1
Switch(dhcpv6-config)#
```

В данном примере показано, как настроить статическую запись привязки адреса в пуле IPv6 DHCP «pool2» с опцией IAID и ассоциировать пул IPv6 DHCP с VLAN 200.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool2
Switch(dhcpv6-config)# address-assignment 2001:AAB8::2:2 00030001050611223344 iaid 1234
Switch(dhcpv6-config)# exit
Switch(config)# interface vlan 200
Switch(config-if)# ipv6 dhcp server pool2
Switch(config-if)#
```

23-3 clear ipv6 dhcp binding

Данная команда используется для удаления записей привязки DHCPv6-сервера.

clear ipv6 dhcp binding {all | *IPV6-PREFIX***}**

Параметры

all	Укажите, чтобы удалить все записи привязки.
IPV6-PREFIX	Укажите, чтобы удалить запись привязки по префиксу.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы удалить записи привязки DHCPv6-сервера. При указании IPv6-префикса будет удалена запись привязки к обозначенному клиенту. Если IPv6-префикс не указан, будут удалены все записи привязки. IPv6-префикс будет возвращен в пул, которому изначально был назначен.

Пример

В данном примере показано, как удалить все записи привязки в таблице привязок DHCPv6-сервера.

```
Switch# clear ipv6 dhcp binding all
Switch#
```

23-4 domain-name

Данная команда используется для назначения имени домена запрашивающему DHCPv6-клиенту. Используйте форму **no**, чтобы удалить настройки имени домена.

domain-name *DOMAIN-NAME*
no domain-name

Параметры

DOMAIN-NAME	Укажите имя домена.

По умолчанию

Нет

Режим ввода команды

DHCPv6 Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы назначить имя домена запрашивающему DHCPv6-клиенту. Можно указать только одно имя домена.

Пример

В данном примере показано, как настроить имя домена в пуле DHCPv6-сервера «pool1».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# domain-name v6domain
Switch(config-dhcp)#
```

23-5 dns-server

Данная команда используется для назначения списка серверов DNS IPv6 запрашивающему IPv6-клиенту. Используйте форму **no**, чтобы удалить DNS-сервер из списка серверов.

dns-server *IPV6-ADDRESS*
no dns-server *IPV6-ADDRESS*

Параметры

IPV6-ADDRESS	Укажите IPv6-адрес DNS-сервера.

По умолчанию

Нет

Режим ввода команды

DHCPv6 Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы присвоить IPv6-адрес DNS-сервера запрашивающему DHCPv6-клиенту. Если необходимо присвоить несколько адресов, введите команду несколько раз.

Пример

В данном примере показано, как настроить сервер DNS IPv6 в пуле DHCPv6-сервера «pool1».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# dns-server 2001:0DB8:3000:3000::42
Switch(config-dhcp)#
```

23-6 ipv6 dhcp excluded-address

Данная команда используется для указания IPv6-адресов, которые DHCPv6-сервер не должен присваивать DHCP-клиентам. Используйте форму **no**, чтобы удалить исключенные IPv6-адреса.

ipv6 dhcp excluded-address *LOW-ADDRESS* [*HIGH-ADDRESS*]
no ipv6 dhcp excluded-address *LOW-ADDRESS* [*HIGH-ADDRESS*]

Параметры

LOW-ADDRESS	Укажите исключенный IPv6-адрес или первый IPv6-адрес в диапазоне исключенных адресов.
HIGH-ADDRESS	(Опционально) Укажите последний IPv6-адрес в диапазоне исключенных адресов.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Сервер DHCPv6 предполагает, что клиенту может быть присвоен любой адрес (кроме IPv6-адреса коммутатора). Используйте данную команду, чтобы исключить присвоение одного IPv6-адреса или диапазона IPv6-адресов. Исключенные адреса могут быть присвоены только пулу/пулам адресов.

Пример

В данном примере показано, как исключить IPv6-адрес 3004:DB8::1:10.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp excluded-address 3004:DB8::1:10
Switch(config)#
```

23-7 ipv6 dhcp pool

Данная команда используется для входа в режим DHCP Pool Configuration Mode и настройки пула IPv6 DHCP. Используйте форму **no**, чтобы удалить пул IPv6 DHCP.

ipv6 dhcp pool *POOL-NAME*
no ipv6 dhcp pool *POOL-NAME*

Параметры

POOL-NAME	Укажите имя пула адресов. Максимально допустимое количество символов – 12.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы войти в режим IPv6 DHCP Pool Configuration Mode и настроить пул IPv6 DHCP. Используйте команду **ipv6 dhcp server**, чтобы включить DHCP IPv6 Server Service на интерфейсе и указать пул IPv6 DHCP, используемый для обслуживания DHCP-запроса, полученного на интерфейсе.

Пример

В данном примере показано, как настроить пул адресов «pool1».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)#
```

23-8 ipv6 dhcp server

Данная команда используется для включения DHCP IPv6 Server Service на интерфейсе. Используйте форму **no**, чтобы отключить DHCP IPv6 Server Service.

ipv6 dhcp server *POOL-NAME* **[rapid-commit] [preference** *VALUE***] [allow-hint]**
no ipv6 dhcp server

Параметры

POOL-NAME	Укажите имя пула IPv6 DHCP, обслуживающего запрос, полученный на интерфейсе.
rapid-commit	(Опционально) Укажите, чтобы получать сетевые настройки от DHCP-сервера посредством быстрого обмена двумя сообщениями вместо стандартных четырех между Requesting Router (RR) и Delegating Router (DR). По умолчанию обмен двумя сообщениями отключен.
preference *VALUE*	(Опционально) Указывает значение предпочтения, которое будет рекламироваться сервером Диапазон от 0 до 255. Значение по умолчанию равно 0. Чем больше значение, тем выше приоритет.
allow-hint	(Опционально) Указывает делегировать префикс на основе подсказки префикса клиентом. По умолчанию подсказка префикса клиентом игнорируется.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить DHCP для IPv6 Server Service на указанном интерфейсе.

Один пул IPv6 DHCP можно ассоциировать с несколькими интерфейсами, при этом с одним интерфейсом можно ассоциировать только один пул IPv6 DHCP. Перед ассоциированием пул необходимо настроить. Для IPv6 Client функции DHCP-Server DHCP-Relay несовместимы на одном интерфейсе.

Стандартный обмен сообщениями между маршрутизаторами DR и RR включает в себя четыре типа сообщений: *SOLICIT, ADVERTISE, REQUEST* и *REPLY*. При использовании параметра **rapid-commit** **ма**ршрутизаторы обмениваются двумя сообщениями вместо четырех. В этом случае маршрутизаторRR 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** и на DR,и на RR.

Пример

В данном примере показано, как создать DHCP-пул «pool1» и использовать его для передачи префиксов, включив DHCP IPv6 Server Service на интерфейсе VLAN 100.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# exit
Switch(config)# interface vlan 100
Switch(config-if)# ipv6 dhcp server pool1
Switch(config-if)#
```

23-9 ipv6 local pool

Данная команда используется для настройки локального пула IPv6-префиксов. Используйте форму **no**, чтобы удалить пул.

ipv6 local pool *POOL-NAME IPV6-PREFIX/ PREFIX-LENGTH ASSIGNED-LENGTH*
no ipv6 local pool *POOL-NAME*

Параметры

POOL-NAME	Укажите имя локального пула IPv6-префиксов. Максимально допустимое количество символов – 12.
IPV6-PREFIX	Укажите адрес IPv6-префикса в локальном пуле.
PREFIX-LENGTH	Укажите длину IPv6-префикса в локальном пуле.
ASSIGNED-LENGTH	Укажите длину префикса, который необходимо делегировать из пула пользователю. Заданная длина не может быть меньше длины префикса.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Локальный пул IPv6-префиксов определяет блок префиксов. Настройте пул с префиксами, которые пересекаются с другими пулами. Чтобы изменить префикс в локальном пуле, удалите локальный пул, а затем создайте его заново. Все префиксы данного пула, которые уже были распределены, будут свободны.

Пример

В данном примере показано, как создать локальный пул IPv6-префиксов «prefix-pool» и использовать локальный пул в DHCP-пуле «pool1».

```
Switch# configure terminal
Switch(config)# ipv6 local pool prefix-pool 3004:DB8::/48 64
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# prefix-delegation pool prefix-pool lifetime 300 200
Switch(config-dhcp)#
```

23-10 prefix-delegation

Данная команда используется для указания префикса, который необходимо делегировать обозначенному клиенту. Используйте форму **no**, чтобы удалить префикс статической привязки.

prefix-delegation *IPV6-PREFIX/PREFIX-LENGTH CLIENT-DUID* **[iaid** *IAID***] [lifetime** *VALID-LIFE-TIME PREFERRED-LIFETIME***]**
no prefix-delegation *IPV6-PREFIX/PREFIX-LENGTH*

Параметры

IPV6-PREFIX	Укажите IPv6-префикс, который необходимо делегировать обозначенному клиенту.
PREFIX-LENGTH CLIENT-DUID	Укажите длину IPv6-префикса.
CLIENT-DUID	Укажите DHCP Unique Identifier (DUID) клиента, которому необходимо делегировать префикс.
iaid *IAID*	(Опционально) Укажите Identity Association Identifier (IAID). IAID используется для обозначения серии префиксов, присвоенных Requesting Router (RR).
lifetime *VALID-LIFE-TIME*	(Опционально) Укажите значение Valid Lifetime (допустимое время жизни) для префикса в секундах. Значение Valid Lifetime должно превышать значение Preferred Lifetime (предпочтительное время жизни). Доступный диапазон значений: от 60 до 4294967295 или до бесконечности. Если значение Lifetime не задано, устанавливается значение Valid

	Lifetime по умолчанию – 2592000 секунд (30 дней).
PREFERRED-LIFETIME	(Опционально) Укажите значение Preferred Lifetime для префикса в секундах. Доступный диапазон значений: от 60 до 4294967295 или до бесконечности. Если значение Lifetime не задано, устанавливается значение Preferred Lifetime по умолчанию – 604800 секунд (7 дней).

По умолчанию

Нет

Режим ввода команды

DHCPv6 Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить статическую запись привязки префикса так, чтобы она указывала префикс, который необходимо делегировать обозначенному клиенту. Для клиента можно настроить несколько статических записей привязки префиксов или IAPD.

Получив запрос от клиента, сервер проверит пул IPv6 DHCP, ассоциированный с полученным интерфейсом. Если сообщение request содержит опцию IAPD и имеются свободные статические записи, настроенные с IAID и соответствующие DUID и IAID сообщения, будут делегированы все соответствующие записи. Если соответствующие записи отсутствуют, но имеются свободные статические записи без указанных IAID, которые соответствуют DUID сообщения, на соответствующую запись будет отправлен ответ. Если в сообщении request отсутствует опция IAID, а в наличии есть свободные статические записи без указанных IAID, которые соответствуют DUID сообщения, на соответствующие записи будет отправлен ответ.

При отсутствии соответствующих записей клиенту будет делегирован префикс из локального пула IPv6-префиксов, указанного в пуле IPv6 DHCP.

Пример

В данном примере показано, как настроить статическую запись привязки префикса в пуле IPv6 DHCP «pool1» и ассоциировать данный пул с VLAN 100.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# prefix-delegation 2001:0DB8::/64 000300010506BBCCDDEE
Switch(config-dhcp)# exit
Switch(config)# interface vlan100
Switch(config-if)# ipv6 dhcp server pool1
Switch(config-if)#
```

23-11 prefix-delegation pool

Данная команда используется для указания локального пула IPv6-префиксов, из которого префиксы могут быть делегированы. Используйте форму **no**, чтобы удалить локальный пул IPv6-префиксов.

prefix-delegation pool *POOL-NAME* **[lifetime** *VALID-LIFETIME PREFERRED-LIFETIME***]**
no prefix-delegation pool *POOL-NAME*

Параметры

POOL-NAME	Укажите имя локального пула IPv6-префиксов.
lifetime *VALID-LIFETIME*	(Опционально) Укажите значение Valid Lifetime (допустимое время жизни) для префикса в секундах. Значение Valid Lifetime должно превышать значение Preferred Lifetime (предпочтительное время жизни). Доступный диапазон значений: от 60 до 4294967295 или до бесконечности. Если значение Lifetime не задано, устанавливается значение Valid Lifetime по умолчанию – 2592000 секунд (30 дней).
PREFERRED-LIFETIME	(Опционально) Укажите значение Preferred Lifetime для префикса в секундах. Доступный диапазон значений: от 60 до4294967295 или до бесконечности. Если значение Lifetime не задано, устанавливается значение Preferred Lifetime по умолчанию - 604800 секунд (7 дней).

По умолчанию

Нет

Режим ввода команды

DHCPv6 Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для указания локального пула IPv6-префиксов в пуле IPv6 DHCP, чтобы делегировать префикс клиентам, обслуживаемым DHCP-пулом. В пуле IPv6 DHCP можно указать только один локальный пул IPv6-префиксов.

Получив запрос от клиента, сервер проверит пул IPv6 DHCP, ассоциированный с полученным интерфейсом. Если статические записи привязки префикса настроены так, чтобы делегировать префикс запрашивающему клиенту, будет делегирован префикс статической привязки. Иначе сервер делегирует префикс из локального пула IPv6-префиксов, указанного для пула IPv6 DHCP.

Пример

В данном примере показано, как настроить локальный пул IPv6-префиксов «prefix-pool», указать данный пул в пуле IPv6 DHCP «pool1» и ассоциировать пул IPv6 DHCP с VLAN 100.

```
Switch# configure terminal
Switch(config)# ipv6 local pool prefix-pool 3004:DB8::/48 64
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# prefix-delegation pool prefix-pool lifetime 300 200
Switch(config-dhcp)# exit
Switch(config)# interface vlan 100
Switch(config-if)# ipv6 dhcp server pool1
Switch(config-if)#
```

23-12 service ipv6 dhcp

Данная команда используется для включения сервера IPv6 DHCP и Relay Service на коммутаторе. Используйте форму **no** для отключения сервера IPv6 DHCP и Relay Service.

service ipv6 dhcp
no service ipv6 dhcp

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы глобально включить сервер IPv6 DHCP и Relay Service на коммутаторе. Чтобы настройки вступили в силу, необходимо отключить, а затем снова включить DHCPv6-сервер.

Пример

В данном примере показано, как включить сервер IPv6 DHCP и Relay Service.

```
Switch# configure terminal
Switch(config)# service ipv6 dhcp
Switch(config)#
```

23-13 show ipv6 dhcp

Данная команда используется для отображения настроек DHCPv6 для интерфейсов.

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

Параметры

INTERFACE-ID	(Опционально) Укажите интерфейс VLAN, для которого необходимо отобразить настройки DHC Pv6.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить DHCPv6 DUID устройства. Используйте команду **show ipv6 dhcp interface**, чтобы отобразить настройки DHCPv6 для интерфейсов. Если ID интерфейса не указан, будут отображены все интерфейсы, на которых включена функция DHCPv6.

Пример

В данном примере показано, как отобразить информацию о DHCPv6 для интерфейса VLAN 1, если на VLAN 1 отключен DHCPv6.

```
Switch# show ipv6 dhcp interface vlan 1

vlan 1 is not in DHCPv6 mode

Switch#
```

В данном примере показано, как отобразить DHCPv6 client для интерфейса VLAN 1, если на VLAN 1 включен DHC Pv6-сервер.

```
Switch# show ipv6 dhcp interface vlan 1

vlan 1 is in server mode
  IPv6 DHCP pool is test
  Preference value: 0
  Hint from client: ignored
  Rapid-Commit is disabled

Switch#
```

23-14 show ipv6 dhcp binding

Данная команда используется для отображения записи привязки IPv6-префикса.

show ipv6 dhcp binding [*IPV6-PREFIX***]**

Параметры

IPV6-PREFIX	(Опционально) Укажите, чтобы отобразить запись привязки.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду для отображения всех привязок префикса клиента DHCPv6 из таблицы привязок, если параметр IPV6 prefix не задан. Если параметр префикса IPV6 задан, отображается только конкретная привязка клиентского префикса для данного префикса.

Пример

В данном примере показано, как отобразить запись привязки IPv6-префикса.

```
Switch# show ipv6 dhcp binding

Client DUID : 00030001aabbcd000001
              address: 1234::2
                       preferred lifetime 200 ,valid lifetime 300

Client DUID : 00030001aabbcd000000
              address: 1234::3
                       preferred lifetime 200 ,valid lifetime 300

Client DUID : 00030001aabbcd000002
              address: 1234::4
                       preferred lifetime 200 ,valid lifetime 300


Total Entries: 3

Switch#
```

23-15 show ipv6 dhcp pool

Данная команда используется для отображения информации о настройках пула DHCPv6-сервера.

show ipv6 dhcp pool [*POOL-NAME*]

Параметры

POOL-NAME	(Опционально) Укажите, чтобы отобразить пул IPv6 DHCP.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

При использовании данной команды без указания параметра *POOL-NAME* будет отображена информация о настройках всех пулов DHCPv6-сервера. При указании параметра *POOL-NAME* будет отображена информация только об указанном пуле.

Пример

В данном примере показано, как отобразить информацию о DHCPv6-пуле.

```
Switch# show ipv6 dhcp pool

DHCPv6 pool: pool1
        Static bindings:
           Binding for client 00030001aabbcd000080
           IA PD: IA ID 0x0001
              Prefix: 3000:0:300::/48
               preferred lifetime 604800, valid lifetime 2592000
        Prefix delegation pool: abc
              preferred lifetime 604800, valid lifetime 2592000
        DNS server: 2345::2
        Domain name: pool1.com
        Active clients: 0

DHCPv6 pool: pool2
        DNS server: 6000::2
        DNS server: 6000::9
        Domain name: pool2.com
        Active clients: 0

DHCPv6 pool: test
        Static bindings:
           Binding for client 00030001aabbcd001234
           IA NA: IA ID not specified
              Address: 1234::1234
               preferred lifetime 604800, valid lifetime 2592000
        Address prefix: 1234::/64
              preferred lifetime 200, valid lifetime 300
        DNS server:
        Domain name:
        Active clients: 3

Switch#
```


Отображаемые параметры

DHCPv6 pool	Имя пула.
Binding for client 000300010002FCA5C01C	Статическая привязка для клиента с DUID 000300010002FCA5C01C.
IAPD	Серия префиксов, присвоенных клиенту.
IAID	Идентификатор данной IAPD.
Prefix	Префиксы, которые необходимо делегировать.
preferred lifetime, valid lifetime	Значения Preferred Lifetime и Valid Lifetime для префикса, присвоенные клиенту.
DNS server	Список адресов DNS-сервера.

Domain name	Список настроенных DNS-доменов.
Active clients	Общее количество активных клиентов.

23-16 show ipv6 excluded-address

Данная команда используется для отображения информации о настройках исключенных IPv6-адресов.

show ipv6 excluded-address

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить диапазон исключенных адресов.

Пример

В данном примере показано, как отобразить исключенные адреса.

```
Switch# show ipv6 excluded-address

 IPv6 excluded address:
        1.      2000::123
        2.      2000::237 - 2000::333

 Total Entries: 2

Switch#
```

23-17 show ipv6 local pool

Данная команда используется для отображения информации о настройках локального пула IPv6-префиксов.

show ipv6 local pool [*POOL-NAME*]

Параметры

POOL-NAME	(Опционально) Укажите, чтобы отобразить локальный пул IPv6 префиксов.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду, чтобы отобразить настройки для определенного локального пула префиксов IPv6 или настройки для всех префиксов, если параметр имени пула не указан.

Пример

В данном примере показано, как отобразить информацию о локальном пуле, не указывая имя пула.

```
Switch#show ipv6 local pool

Pool         Prefix                                    Free In use
------------ ----------------------------------------- ---- ------
prefix-pool  3004:DB8::/48                             65536 0
------------ ----------------------------------------- ---- ------
Total Entries: 1

Switch#
```

В данном примере показано, как отобразить информацию о локальном пуле «PP1».

```
Prefix is 3004:DB8::/48 assign /64 prefix
1 entries in use, 65536 available, 0 rejected
User                Prefix                                    Interface
------------------- ----------------------------------------- ----------
000300010002FCA5C01C 2003::/64                                vlan 1

Switch#
```

23-18 show ipv6 dhcp operation

Данная команда используется для того, чтобы отобразить эксплуатационные данные для DHCPv6-сервера.

show ipv6 dhcp operation

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить эксплуатационные данные для DHCPv6-сервера.

Пример

В данном примере показано, как отобразить эксплуатационные данные для DHCPv6-сервера.

```
Switch# show ipv6 dhcp operation

DHCPv6 pool: pool1
        Prefix delegation pool: abc, prefix is 3000::/32 48
        Static bindings:
           Binding for client 00030001aabbcd000080
             IA PD: IA ID 0x0001
             Prefix: 3000:0:300::/48
             preferred lifetime 604800, valid lifetime 2592000
        preferred lifetime 604800, valid lifetime 2592000
        DNS server: 2345::2
        Domain name: pool1.com

DHCPv6 pool: test
        Address prefix: 1234::/64
        Static bindings:
           Binding for client 00030001aabbcd001234
            IA NA: IA ID not specified
              Address: 1234::1234
               preferred lifetime 604800, valid lifetime 2592000
        preferred lifetime 200, valid lifetime 300
        DNS server: 2000::2
        Domain name: test.com

switch#
```

24. Команды Digital Diagnostics Monitoring (DDM)

24-1 show interfaces transceiver

Данная команда используется для отображения текущих операционных параметров модуля SFP/SFP+.

show interfaces [*INTERFACE-ID* **[, | -] transceiver [detail]**

Параметры

INTERFACE-ID	(Опционально) Укажите интерфейсы, для которых необходимо отобразить статус Transceiver Monitoring. Если interface ID не указаны, будут отображены статусы Transceiver Monitoring для всех действующих интерфейсов.
,	(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.
detail	(Опционально) Укажите, чтобы отобразить более подробнуюинформацию.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить текущие операционные параметры Transceiver Monitoring для модуля SFP/SFP+ на указанных портах.

Пример

В данном примере показано, как отобразить текущие операционные параметры для всех портов, поддерживающих функцию Transceiver Monitoring.

В данном примере показано, как отобразить подробную информацию Transceiver Monitoring для всех портов, поддерживающих данную функцию.

```
Switch#show interfaces transceiver

 ++ : high alarm, +  : high warning, -  : low warning, -- : low alarm
 mA: milliamperes, mW: milliwatts

Transceiver Monitoring traps: None

 Port    Temperature   Voltage    Bias Current   TX Power     RX Power
           (Celsius)     (V)         (mA)          (mW)         (mW)
------- ------------ ----------- ------------ ------------ ------------
eth2/0/23     30.090     3.353      16.794(++)    0.258       0.000(--)
eth3/0/25     29.316     3.302       5.326        0.529       0.506
eth3/0/26     31.617     3.297       5.170        0.527       0.504

Total Entries: 3

Switch#
```

В данном примере показано, как отобразить подробную информацию Transceiver Monitoring для всех портов, поддерживающих данную функцию.

```
Switch# show interfaces transceiver detail

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm
mA: milliamperes, mW: milliwatts
A: The threshold is administratively configured.

eth2/0/3
Transceiver Monitoring is enabled
Transceiver Monitoring shutdown action：Alarm

                  Current     High-Alarm  High-Warning Low-Warning Low-Alarm
Temperature(C)    30.090      75.000(A)   70.000       0.000       -5.000
Voltage (v)        3.353       3.630       3.465       3.135        2.970
Bias Current(mA)  16.794(++)  10.500       9.000       2.500        2.000
TX Power (mW)      0.258       1.413       0.708       0.186        0.074
RX Power (mW)      0.000(--)   1.585       0.794       0.102        0.041

Switch#
```

24-2 snmp-server enable traps transceiver-monitoring

Данная команда используется для того, чтобы включить отправку всех или определенных SNMP-уведомлений Optical Transceiver Monitoring. Используйте форму **no**, чтобы отключить отправку уведомлений.

snmp-server enable traps transceiver-monitoring [alarm] [warning]

no snmp-server enable traps transceiver-monitoring [alarm] [warning]

Параметры

alarm	(Опционально) Укажите, чтобы включить/отключить отправкууведомлений уровня alarm (тревога).
warning	(Опционально) Укажите, чтобы включить/отключить отправкууведомлений уровня warning (предупреждение).

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для отправки всех или указанного уровня SNMP-уведомлений о мониторинге трансивера.

Пример

В данном примере показано, как включить отправку уведомлений уровня warning.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps transceiver-monitoring warning
Switch(config)#
```

24-3 transceiver-monitoring action shutdown

Используйте данную команду, чтобы отключить порт при обнаружении события alarm (тревога) или warning (предупреждение). Используйте форму **no**, чтобы отключить данную функцию.

transceiver-monitoring action shutdown {alarm | warning}
no transceiver-monitoring action shutdown

Параметры

alarm	Укажите, чтобы отключить порт при обнаружении события alarm.
warning	Укажите, чтобы отключить порт при обнаружении события warning.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить интерфейс физического порта.

Данная команда позволяет указать, будет ли отключаться порт при обнаружении события alarm / события warning. Если функция Monitoring включена, отслеживаются события alarm и события warning. Событие alarm происходит, если отслеживаемые параметры выходят за пределы верхнего или нижнего порога alarm. Событие warning происходит, если отслеживаемые параметры выходят за пределы верхнего или нижнего порога warning.

Отключение порта контролируется модулем Error Disable без таймера Recover. Пользователь может включить порт вручную, применив команду **shutdown**, а затем команду **no shutdown**.

Пример

В этом примере показано, как настроить отключение интерфейса eth3/0/1 при обнаружении тревожного события.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# transceiver-monitoring action shutdown alarm
Switch(config-if)#
```

24-4 transceiver-monitoring bias-current

Данная команда используется для настройки порогов тока смещения на указанном порту. Используйтеформу **no**, чтобы удалить заданные настройки.

transceiver-monitoring bias-current *INTERFACE-ID* **{high | low} {alarm | warning}** *VALUE*
no transceiver-monitoring bias-current *INTERFACE-ID* **{high | low} {alarm | warning}**

Параметры

INTERFACE-ID	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.
low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
VALUE	Укажите порог в диапазоне от 0 до 131 мА.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данный функционал доступен только для интерфейсов портов SFP+ с оптическими модулями, поддерживающими функцию Transceiver Monitoring.

Данная команда позволяет настроить пороги тока смещения на указанных портах. Заданные значения сохраняются как в системе, так и в трансиверах SFP/SFP+, а также будут направлены в модуль SFP/SFP+ в 16-битном формате.

Если конфигурируемый модуль SFP/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен в системе и отображен. При отсутствии пороговых значений, заданных пользователем, будут отображены значения, заданные производителем.

При помощи формы **no** данной команды можно удалить заданные пороговые значения, сохраненные в системе. При этом пороговые значения, сохраненные в трансиверах SFP/SFP+, остаются неизменными. Используйте форму **no**, чтобы предотвратить изменения пороговых значений в трансивере SFP/SFP+ при его первом подключении.

Пример

В этом примере показано, как настроить порог предупреждения о высоком токе смещения как 10.237 на интерфейсе eth1/0/25.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring bias-current eth1/0/25 high warning 10.237

WARNING: A closest value 10.236 is chosen according to the transceiver-monitoring
precision definition.

Switch(config)#
```

24-5 transceiver-monitoring enable

Данная команда используется для включения функции Optical Transceiver Monitoring на порту SFP+. Используйте форму **no**, чтобы отключить функцию Optical Transceiver Monitoring.

transceiver-monitoring enable
no transceiver-monitoring enable

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить интерфейс физического порта.

Данная команда позволяет включить/отключить функцию Optical Transceiver Monitoring на порту SFP+. Если функция Monitoring включена, отслеживаются события alarm и события warning. Событие alarm происходит, если отслеживаемые параметры выходят за пределы верхнего или нижнего порога alarm. Событие warning происходит, если отслеживаемые параметры выходят за пределы верхнего или нижнего порога warning.

Если трансивер SFP/SFP+ с функцией transceiver monitoring подключен к порту, на котором данная функция отключена, система не сможет определить аварийный статус трансивера SFP/SFP+, однако пользователь может проверить статус при помощи команды interface transceiver.

Пример

В этом примере показано, как включить мониторинг трансивера на интерфейсе eth3/0/1.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# transceiver-monitoring enable
Switch(config-if)#
```

24-6 transceiver-monitoring rx-power

Данная команда используется для настройки порогов входной мощности на указанном порту. Используйте форму **no**, чтобы удалить заданные настройки.

transceiver-monitoring rx-power *INTERFACE-ID* **{high | low} {alarm | warning} {mwatt** *VALUE* **|dbm** *VALUE***}**

no transceiver-monitoring rx-power *INTERFACE-ID* **{high | low} {alarm | warning}**

Параметры

INTERFACE-ID	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.

low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
mwatt *VALUE*	Укажите порог входной мощности в диапазоне от 0 до 6,5535 мВт.
dbm *VALUE*	Укажите порог входной мощности в диапазоне от -40 до 8,1647 дБм.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данный функционал доступен только для интерфейсов портов SFP+ с оптическими модулями, поддерживающими функцию Transceiver Monitoring.

Данная команда позволяет настроить пороги входной мощности на указанном порту. Заданные значения сохраняются как в системе, так и в трансиверах SFP/SFP+, а также будут направлены в модуль SFP/SFP+ в 16-битном формате.

Если конфигурируемый модуль SFP/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен в системе и отображен. При отсутствии пороговых значений, заданных пользователем, будут отображены значения, заданные производителем.

При помощи формы **no** данной команды можно удалить заданные пороговые значения, сохраненные в системе. При этом пороговые значения, сохраненные в трансиверах SFP/SFP+, остаются неизменными. Используйте форму **no**, чтобы предотвратить изменения пороговых значений в трансивере SFP/SFP+ при его первом подключении.

Пример

В этом примере показано, как настроить порог предупреждения о низком уровне мощности RX как 0,135 мВт на интерфейсе eth3/0/1.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring rx-power eth3/0/1 low warning mwatt 0.135
Switch(config)#
```

24-7 transceiver-monitoring temperature

Данная команда используется для настройки порогов температуры на указанном порту. Используйте форму **no**, чтобы удалить заданные настройки.

transceiver-monitoring temperature *INTERFACE-ID* **{high | low} {alarm | warning}** *VALUE*
no transceiver-monitoring temperature *INTERFACE-ID* **{high | low} {alarm | warning}**

Параметры

INTERFACE-ID	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.
low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
VALUE	Укажите порог температуры в диапазоне от -128 до +127,996 °C.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данный функционал доступен только для интерфейсов портов SFP+ с оптическими модулями, поддерживающими функцию Transceiver Monitoring.

Данная команда позволяет настроить пороги температуры на указанном порту. Заданные значения сохраняются как в системе, так и в трансиверах SFP/SFP+, а также будут направлены в модуль SFP/SFP+ в 16-битном формате.

Если конфигурируемый модуль SFP/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен в системе и отображен. При отсутствии пороговых значений, заданных пользователем, будут отображены значения, заданные производителем.

При помощи формы no данной команды можно удалить заданные пороговые значения, сохраненные в системе, при этом пороговые значения, сохраненные в трансиверах SFP/SFP+, остаются неизменными. Используйте форму no, чтобы предотвратить изменения пороговых значений в трансивере SFP/SFP+ при его первом подключении.

Пример

В этом примере показано, как настроить порог сигнала тревоги о высокой температуре как 127.994 на интерфейсе eth3/0/1.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring temperature eth3/0/1 high alarm 127.994

 WARNING: A closest value 127.992 is chosen according to the transceiver-monitoring
precision definition.
Switch(config)#
```

24-8 transceiver-monitoring tx-power

Данная команда используется для настройки порогов выходной мощности на указанном порту. Используйте форму **no**, чтобы удалить заданные настройки.

transceiver-monitoring tx-power *INTERFACE-ID* **{high | low} {alarm | warning} {mwatt** *VALUE* **|dbm** *VALUE***}**

no transceiver-monitoring tx-power *INTERFACE-ID* **{high | low} {alarm | warning}**

Параметры

INTERFACE-ID	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.
low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
mwatt *VALUE*	Укажите порог выходной мощности в диапазоне от 0 до 6,5535 мВт.
dbm *VALUE*	Укажите порог выходной мощности в диапазоне от -40 до 8,1647 дБм.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данный функционал доступен только для интерфейсов портов SFP+ с оптическими модулями, поддерживающими функцию Transceiver Monitoring.

Данная команда позволяет настроить пороги выходной мощности на указанных портах. Заданные значения сохраняются как в системе, так и в трансиверах SFP/SFP+, а также будут направлены в модуль SFP/SFP+ в 16-битном формате.

Если конфигурируемый модуль SFP/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен в системе и отображен. При отсутствии пороговых значений, заданных пользователем, будут отображены значения, заданные производителем.

При помощи формы **no** данной команды можно удалить заданные пороговые значения, сохраненные в системе. При этом предельные значения, сохраненные в трансиверах SFP/SFP+, остаются неизменными. Используйте форму **no**, чтобы предотвратить изменения пороговых значений в трансивере SFP/SFP+ при его первом подключении.

Пример

В этом примере показано, как настроить порог предупреждения о низком уровне мощности TX на 0,181 мВт на интерфейсе eth3/0/1.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring tx-power eth3/0/1 low warning mwatt 0.181
Switch(config)#
```

24-9 transceiver-monitoring voltage

Данная команда используется для настройки порогов напряжения на указанном порту. Используйте форму **no**, чтобы удалить заданные настройки.

transceiver-monitoring voltage *INTERFACE-ID* **{high | low} {alarm | warning}** *VALUE*
no transceiver-monitoring voltage *INTERFACE-ID* **{high | low} {alarm | warning}**

Параметры

INTERFACE-ID	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.
low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
VALUE	Укажите порог напряжения в диапазоне от 0 до 6,5535 В.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данный функционал доступен только для интерфейсов портов SFP+ с оптическими модулями, поддерживающими функцию Transceiver Monitoring.

Данная команда позволяет настроить пороги напряжения на указанных портах. Заданные значения сохраняются как в системе, так и в трансиверах SFP/SFP+, а также будут направлены в модуль SFP/SFP+ в 16-битном формате.

Если конфигурируемый модуль SFP/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен в системе и отображен. При отсутствии пороговых значений, заданных пользователем, будут отображены значения, заданные производителем.

При помощи формы **no** данной команды можно удалить заданные пороговые значения, сохраненные в системе. При этом пороговые значения, сохраненные в трансиверах SFP/SFP+, остаются неизменными. Используйте форму **no**, чтобы предотвратить изменения предельных значений в трансивере SFP/SFP+ при его первом подключении.

Пример

В этом примере показано, как настроить порог низкого напряжения тревоги как 0.005 В на интерфейсе eth3/0/1.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring voltage eth3/0/1 low alarm 0.005
Switch(config)#
```

25. Команды клиента D-Link Discovery Protocol (DDP)

25-1 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 отключена.

Режим ввода команды

Global Configuration Mode
Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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 данном примере показано, как включить DDP на порту 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ddp
Switch(config-if)#
```

25-2 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

По умолчанию этот параметр равен 30 секундам.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

25-3 show ddp

Данная команда используется для отображения настроек DDP на коммутаторе.

show ddp [interfaces {*INTERFACE-ID* **[, | -]}]**

Параметры

INTERFACE-ID	Укажите interface ID.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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
Report timer: 60 seconds

Switch#
```

В данном примере показано, как отобразить информацию о DDP на порту 1/0/1.

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

Interface         State
--------------    ----------
eth1/0/1          Enabled

Switch#
```

26. Команды Domain Name System (DNS)

26-1 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

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#
```

26-2 ip domain lookup

Данная команда используется для включения DNS, что позволяет использовать функцию Domain Name Resolution. Используйте форму **no**, чтобы отключить данную функцию.

ip domain lookup
no ip domain lookup

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду **ip domain lookup**, 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)#
```

26-3 ip host

Данная команда используется для настройки статической записи привязки для имени узла, а также IP-адреса в таблице узлов. Используйте форму **no**, чтобы удалить статическую запись узла.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Имя узла, указанное в этой команде, должно быть подходящим. Чтобы удалить статическую запись узла, используйте форму no данной команды.

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)#
```

26-4 ip name-server

Данная команда используется для настройки IP-адреса Domain Name Server. Используйте форму **no**, чтобы удалить сконфигурированный Domain Name Server.

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 несколько IP-адресов, разделяя их при помощи пробелов. Можно указать не более 2 серверов.
IPV6-ADDRESS2	Укажите несколько IPv6-адресов, разделяя их при помощи пробелов. Можно указать не более 2 серверов.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для настройки сервера DNS. Если система не может получить ответ от DNS-сервера, она будет пытаться использовать следующий сервер до тех пор, пока не получит ответ. Если серверы имен уже настроены, серверы, настроенные позже, будут добавлены в список серверов. Можно указать два сервера имен 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)#
```

26-5 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 указанногоName Server. Доступный диапазон значений: от 1 до 60 секунд.

По умолчанию

Значение по умолчанию – 3 секунды.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

26-6 show hosts

Данная команда используется для отображения настроек DNS.

show hosts

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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
 TTL:                forever


Switch#
```

Отображаемые параметры

TTL	Укажите максимальное время ожидания ответа от указанногоName Server. Доступный Значение Time-To-Leave (TTL) отображается, когда запись является динамическая запись. Ключевое слово "навсегда" отображается, если запись является статической записью значений: от 1 до 60 секунд.

26-7show ip name-server

Данная команда используется для отображения текущих DNS.

show ip name-server

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить DNS.

Пример

В этом примере показано, как отобразить конфигурацию DNS, когда записи динамического сервера имен были получены от сервера DHCP.

```
Switch#show ip name-server

 Static name server:
 192.168.5.134
 5001:5::2

 Dynamic name server:
 1.1.1.1
 1.1.1.2

Switch#
```

В этом примере показано, как отобразить конфигурацию DNS, когда от сервера DHCP не было получено ни одной записи динамического сервера имен.

```
Switch#show ip name-server

 Static name server:
 192.168.5.134
 5001:5::2

 Dynamic name server:

Switch#
```

27. Команды предотвращения атак DoS

27-1 dos-prevention

Данная команда используется для включения и настройки механизма предотвращения атак DoS (DoS Prevention). При использовании формы **no** данная команда вернется к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения и настройки механизма предотвращения атак DoS для определенного типа атак DoS или для 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 кзначениям 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-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)#
```

27-2 show dos-prevention

Данная команда используется для получения информации о статусе предотвращения атак DoS и соответствующих счетчиках.

show dos-prevention [*DOS-ATTACK-TYPE***]**

Параметры

DOS-ATTACK-TYPE	(Опционально) Укажите тип DoS, который необходимо отобразить.

По умолчанию

Нет

Режим ввода команды

User-Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для получения информации о статусе предотвращения атак DoS.

Пример

В данном примере показан процесс вызова информации о настройках предотвращения атак DoS.

```
Switch#show dos-prevention

DoS Prevention Information
DoS Type                    State
--------------------------- --------
Land Attack                 Enabled
Blat Attack                 Enabled
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 показан процесс вызова информации о настройках предотвращения атак DoS для типа атаки Land.

```
Switch#show dos-prevention land

DoS Type : Land Attack
State    : Enabled

Switch#
```

27-3 snmp-server enable traps dos-prevention

Данная команда используется для отправки SNMP-уведомлений о DoS-атаках. Для отключения данной команды используйте форму **no**.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Если предотвращение атак DoS включено, каждые пять минут коммутатор будет записывать в журнал событие, 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 трапов для атак DoS.

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

28. Команды Dynamic ARP Inspection

28-1 arp access-list

Данная команда используется для создания или изменения списка доступа ARP. Команда позволяет войти в режим ARP Access-list Configuration Mode. При использовании формы **no** данная команда удалит список доступа ARP.

arp access-list *NAME*
no arp access-list *NAME*

Параметры

NAME	Укажите имя списка доступа ARP, который необходимо настроить. Максимальная допустимая длина – 32 символа.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

28-2 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

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#
```

28-3 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 для удаления данных статистики Dynamic ARP Inspection для всех VLAN.
vlan *VLAN-ID*	Укажите VLAN или диапазон VLAN.
,	(Опционально) Выделение серии VLAN или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Выделение диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

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#
```

28-4 ip arp inspection filter vlan

Данная команда используется для указания списка доступа ARP, который будет использоваться для проверки ARP Inspection для VLAN. При использовании формы **no** команда удалит указанную привязку.

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	Указывает имя списка управления доступом. Максимальная допустимая длина – 32 символа.
vlan *VLAN-ID*	Укажите VLAN, сопоставленную со списком доступа ARP.
,	(Опционально) Выделение серии VLAN или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Выделение 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется 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 привязки DHCP Snooping. Проверка будет производиться, если данная команда сконфигурирована.

Списки управления доступом ARP (ARP ACL) имеют более высокий приоритет над таблицей привязки 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)#
```

28-5 ip arp inspection limit

Данная команда используется для ограничения скорости входящих ARP-запросов и ответов на интерфейсе. При использовании формы **no** команда вернется к значениям по умолчанию.

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. Доступен диапазон значений от 1 до 150.
burst interval *SECONDS*	(Опционально) Укажите разрешенную величину продолжительности всплеска (burst duration) ARP-пакетов. Доступен 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 синтервалом всплеска burst interval в 1 секунду.
Для доверенных интерфейсов DAI ограничений нет.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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 ethernet 1/0/10
Switch(config-if)# ip arp inspection limit rate 30 burst interval 5
Switch(config-if)#
```

28-6 ip arp inspection log-buffer

Данная команда используется для настройки параметра буфера журнала ARP Inspection.

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

Уровень команды по умолчанию

Уровень 12

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 через 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)#
```

28-7 ip arp inspection trust

Данная команда используется для назначения доверенного интерфейса для Dynamic ARP Inspection. При использовании формы **no** команда отключит режим доверенного интерфейса.

ip arp inspection trust
no ip arp inspection trust

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 порта 1/0/3 для DAI.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ip arp inspection trust
Switch(config-if)#
```

28-8 ip arp inspection validate

Данная команда используется для указания дополнительных проверок при ARP Inspection. При использовании формы **no** команда отключит дополнительные проверки.

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 ARP заголовке.
dst-mac	(Опционально) Укажите для проверки пакетов ARP-ответов, а также согласованности MAC-адреса источника в заголовке Ethernet с MAC-адресом источника в ARP заголовке.
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, а также 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

Уровень команды по умолчанию

Уровень 12

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 никакие параметры не указаны, все опции включены или выключены. При использовании формы no команда отключит дополнительные типы проверок.

Пример

В данном примере показано, как включить проверку MAC-адреса источника.

```
Switch# configure terminal
Switch(config)# ip arp inspection validate src-mac
Switch(config)#
```

28-9 ip arp inspection vlan

Данная команда используется для включения Dynamic ARP Inspection для определенных VLAN. При использовании формы **no** команда отключит Dynamic ARP Inspection для VLAN.

ip arp inspection vlan *VLAN-ID* **[, | -]**
no ip arp inspection vlan *VLAN-ID* **[, | -]**

Параметры

vlan *VLAN-ID*	Укажите VLAN, для которой необходимо включить или отключить функцию ARPInspection.
,	(Опционально) Выделение серии или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию ARP Inspection отключена для всех VLAN.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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, либо таблицей привязки DHCP Snooping, ARP-пакеты будут отброшены. Помимо проверки привязки адреса, осуществляться будет 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)#
```

28-10 ip arp inspection vlan logging

Данная команда используется для управления типом пакетов, которые будут регистрироваться (логироваться). При использовании формы **no** команда вернется к значениям по умолчанию.

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) Выделение серии или разделение группы

	VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон 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).
permit	Укажите для логирования, разрешенного сконфигурированным списком управления доступом (ACL).
all	Укажите для логирования, разрешенного или запрещенного сконфигурированным списком управления доступом (ACL).
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.
permit	Укажите для логирования, разрешенного привязкой DHCP.
all	Укажите для логирования, разрешенного или запрещенного привязкой DHCP.
none	Укажите, чтобы отменить логирование всех пакетов, разрешенных или запрещенных на основе привязки DHCP.

По умолчанию

Все запрещенные и отброшенные пакеты логируются.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте форму **no**, чтобы команда вернулась к критериям логирования по умолчанию.

Пример

В данном примере показано, как настроить ARP Inspection во 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)#
```

28-11 permit | deny (arp access-list)

Данная команда используется для управления доступом ARP-записи. Используйте команду **deny** для создания запрещающей ARP-записи. При использовании формы **no** команда удалит запись.

{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	Укажите IP-адрес источника.
any	Укажите для сопоставления любого IP-адреса источника.
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	Укажите MAC-адрес.
any	Укажите для сопоставления любого MAC-адреса источника.
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

Уровень команды по умолчанию

Уровень 12

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)#
```

28-12 show ip arp inspection

Данная команда используется для отображения статуса DAI для указанного диапазона VLAN.

show ip arp inspection [interface *INTERFACE-ID* **[, | -]] statistics [vlan** *VLAN-ID* **[, | -]]]**

Параметры

interface *INTERFACE-ID*	(Опционально) Интерфейс (порт), группа интерфейсов (портов) или все интерфейсы (порты), которые необходимо настроить
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятойнедопустимы.
-	(Опционально) Выделение диапазона интерфейсов. Пробелы до ипосле дефиса недопустимы.
statistics	(Опционально) Указывает данные статистики DAI.
vlan *VLAN-ID*	(Опционально) Укажите VLAN или группу VLAN.
,	(Опционально) Выделение серии VLAN или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Выделение диапазона VLAN. Пробелы до и последефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения статуса 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 которой 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 привязки 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      : Enabled
Destination MAC Validation: Disabled
IP Address Validation      : Disabled
VLAN State    ACL Match                          Static ACL
---- -------- ---------------------------------- ----------
10   Disabled static-arp-list                    No
VLAN ACL Logging DHCP Logging
---- ----------- ------------
10   Deny        Deny

Switch#
```

Отображаемые параметры

VLAN	VLAN ID, на которой действует ARP Inspection.
State	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 основесовпадения 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 управлениядоступом (ACL).
DHCP Logging	Состояние логирования для пакетов, отброшенных или разрешенных на основетаблицы привязки DHCP. **None**: пакеты, отброшенные или разрешенные таблицей привязки DHCP, нелогируются. **Permit**: логирование происходит, если пакеты разрешены таблицей привязкиDHCP. **Deny**: логирование происходит, если пакеты отброшены таблицей привязки DHCP. **All**: пакеты, отброшенные или разрешенные таблицей привязки DHCP, логируются.

Пример

В этом примере показано, как отобразить состояние доверия для интерфейса eth3/0/3.

```
Switch# show ip arp inspection interfaces eth3/0/3

Interface   Trust State   Rate(pps)  Burst Interval
---------   -----------   ---------  --------------
eth3/0/3     untrusted     30            5

Switch#
```

В данном примере показано, как включить отображение состояний для интерфейсов коммутатора.

```
Switch# show ip arp inspection interfaces

Interface   Trust State   Rate(pps)    Burst Interval
---------   -----------   ---------   -------------
eth3/0/1      untrusted    30            1
eth3/0/2      untrusted    30            1
eth3/0/3      untrusted    30            5
eth3/0/5      trusted      None          1
eth3/0/6      untrusted    30            1
eth3/0/7      untrusted    30            1
eth3/0/8      untrusted    30            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, всеARP-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.

28-13 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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: 64

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	MAC-адрес источника у логируемого ARP.
Occurence	Счетчик общего числа логирования записей, а также времени последнего случившегося логирования.

29. Команды Error Recovery

29-1 errdisable recovery

Данная команда используется для включения функции Error Recovery (восстановление 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 | bpdu-protect | arp-rate |dhcp-rate | loopback-detect} [interval *SECONDS***]**

no errdisable recovery cause {all | psecure-violation | storm-control | bpdu-protect | arp-rate |dhcp-rate | loopback-detect | l2pt-guard | duld} [interval *SECONDS***]**

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.
bpdu-protect	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной BPDU Protection.
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 приошибке, 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Ошибка на порту может быть вызвана Port Security Violations, Storm Control и так далее. При возникновении ошибки порт отключается, однако для настроек конфигурации будет действоватьопция **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)#
```

29-2 show errdisable recovery

Данная команда используется для отображения настроек Recovery Timer (таймер восстановления).

show errdisable recovery

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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
BPDU Attack Protection              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#
```

29-3 snmp-server enable traps errdisable

Эта команда используется для включения отправки SNMP-уведомлений для отключенного состояния ошибки. Используйте форму **no** этой команды, чтобы отключить отправку SNMP-уведомлений.

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 включить/отключить отправку SNMP-уведомлений об ошибке на порту.
cleared	(Опционально) Укажите, чтобы включить/отключить отправку SNMP-уведомлений об устранении ошибки.
notification-rate *TRAP-RATE*	(Опционально) Укажите количество трапов 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда с параметрами **asserted** и **cleared** включает или отключает уведомления об изменении состояния error disabled. Если вы вводите команду с одним из параметров, включается или отключается только указанный тип уведомления. Состояние или значение другого типа уведомлений не затрагивается.

Команды **snmp-server enable traps errdisable notification-rate** и **no snmp-server enable traps errdisable notification-rate** влияют только на настройку notification-rate, но не на состояние отправки уведомлений для состояния error disabled.

Пример

В этом примере показано, как включить отправку ловушек для входа в состояние error disabled и выхода из него и установить максимальное количество ловушек в секунду равным 3.

```
Switch# configure terminal
Switch(config)#snmp-server enable traps errdisable asserted cleared notification-
rate 3
Switch(config)#
```

30. Команды Ethernet Ring Protection Switching (ERPS)

Более подробную информацию см. в **Приложении E - Информация о ERPS**.

30-1 description

Эта команда используется для настройки описания для экземпляров Ethernet Ring Protection (ERP).

description *DESCRIPTION*

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для настройки описания для экземпляров ERP.

Пример

В этом примере показано, как настроить описание для экземпляров ERP.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#description major-ring instance 1
Switch(config-erps-ring-instance)#
```

30-2 ethernet ring g8032

Эта команда используется для создания или изменения физического кольца ITU-T G.8032 ERP и входа в режим конфигурации ERP. Для удаления указанного кольца используйте форму **no** этой команды.

ethernet ring g8032 *RING-NAME*
no ethernet ring g8032 *RING-NAME*

Параметры

RING-NAME	Указывает имя кольца ERP с максимальным количеством символов 32.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для создания, изменения или удаления физического кольца ERP ITU-T G.8032 и входа в режим конфигурации ERP.

Пример

В этом примере показано, как создать кольцо ERP с именем "campus".

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 campus
Switch(config-erp)#
```

30-3 ethernet ring g8032 profile

Данная команда используется для создания профиля G.8032 и входа в режим G.8032 Profile Configuration Mode. Используйте форму **no**, чтобы удалить профиль G.8032.

ethernet ring g8032 profile *PROFILE-NAME*
no ethernet ring g8032 profile *PROFILE-NAME*

Параметры

PROFILE-NAME	Укажите имя профиля G.8032. Максимально допустимое количество символов – 32.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы создать или изменить профиль G.8032 и войти в режим G.8032 Profile Configuration Mode.

Пример

В данном примере показано, как создать профиль G.8032 «campus».

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 profile campus
Switch(config-g8032-ring-profile)#
```

30-4 tcn-propagation

Данная команда используется для включения передачи уведомлений об изменении топологии (TCN) от экземпляра sub-ERPS к основному экземпляру. Используйте форму **no**, чтобы отключить передачу уведомлений об изменении топологии.

tcn-propagation
no tcn-propagation

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

G.8032 Profile Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить передачу уведомлений об изменении топологии от экземпляра подкольца к другим экземплярам кольца.

Пример

В данном примере показано, как включить передачу TCN для профиля G.8032 «campus».

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 profile campus
Switch(config-erps-ring-profile)#tcn-propagation
Switch(config-erps-ring-profile)#
```

30-5 r-aps channel-vlan

Данная команда используется для настройки ERPS R-APS VLAN. Используйте форму **no**, чтобы удалить настройки.

r-aps channel-vlan *VLAN-ID*
no r-aps channel-vlan

Параметры

VLAN-ID	Укажите ID R-APS VLAN для экземпляра ERPS. Доступный диапазон значений: от 1 до 4094.

По умолчанию

Нет

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для назначения VLAN канала APS для экземпляра ERP. APS-канал VLAN должен быть назначен до того, как экземпляр ERP может быть переведен в рабочее состояние.

Указанная сеть VLAN канала APS не обязательно должна существовать для настройки этой команды. Но она должна существовать до того, как экземпляр будет переведен в рабочее состояние.

Если VLAN канала APS будет удалена, когда экземпляр ERP находится в рабочем состоянии, экземпляр ERP перейдет в состояние отключения работы.

Каждый экземпляр ERP должен иметь отдельную сеть VLAN канала APS.

VLAN канала APS экземпляра подкольца также является виртуальным каналом подкольца.

Пример

В этом примере показано, как настроить VLAN канала APS "2" для экземпляра ERP "1".

```
Switch(config)#ethernet ring g8032 ring1
Switch(config-erp)#instance 1
Switch(config-erp-instance)#r-aps channel-vlan 2
Switch(config-erp-instance)#
```

30-6 inclusion-list vlan-ids

Данная команда используется для определения заданных VLAN ID, которые защищены механизмом Ethernet Ring Protection. Используйте форму **no**, чтобы удалить заданные VLAN ID.

inclusion-list vlan-ids *VLAN-ID* **[, | -]**
no inclusion-list vlan-ids *VLAN-ID* **[, | -]**

Параметры

VLAN-ID	Укажите VLAN ID защищенных VLAN экземпляра ERPS. Доступный 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

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для добавления или удаления идентификаторов VLAN, защищенных механизмом ERP.

Пример

В этом примере показано, как настроить защищаемую службой VLAN как 100-200 для экземпляра ERP 1.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erp)#instance 1
Switch(config-erp-instance)#inclusion-list vlan-ids 100-200
Switch(config-erp-instance)#
```

30-7 instance

Данная команда используется для создания экземпляра ERPS и входа в режим ERPS Instance Configuration Mode. Используйте форму **no**, чтобы удалить экземпляр ERPS.

instance *INSTANCE-ID*
no instance *INSTANCE-ID*

Параметры

INSTANCE-ID	Укажите идентификатор экземпляра ERPS в диапазоне от 1 до 32.

По умолчанию

Нет

Режим ввода команды

ERPS Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для создания или удаления экземпляра ERP и входа в режим конфигурации экземпляра ERP.

Пример

В этом примере показано, как создать экземпляр ERP "1" в физическом кольце с именем "ring2".

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erp)#instance 1
Switch(config-erp-instance)#
```

30-8 level

Данная команда используется для настройки значения MEL кольца экземпляра ERP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

level *MEL-VALUE*
no level

Параметры

MEL-VALUE	Укажите значение MEL кольца экземпляра ERPS в диапазоне от 0 до 7.

По умолчанию

Значение по умолчанию – 1.

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для настройки значения MEL кольца экземпляра ERP. Настроенное значение MEL всех узлов кольца, участвующих в одном экземпляре ERP, должно быть одинаковым.

Пример

В данном примере показано, как настроить значение MEL кольца ERPS-экземпляра 1. Указанное значение – 6.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erp)#instance 1
Switch(config-erp-instance)#level 6
Switch(config-erp-instance)#
```

30-9 sub-ring

Данная команда используется для указания экземпляра подкольца по умолчанию экземпляра для физического экземпляра кольца по умолчанию. Используйте форму **no**, чтобы удалить экземпляр подкольца по умолчанию.

sub-ring *SUB-RING-NAME*
no sub-ring *SUB-RING-NAME*

Параметры

SUB-RING-NAME	Укажите имя подкольца.

По умолчанию

Нет

Режим ввода команды

ERPS Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Настройте подкольцо, подключенное к другому кольцу. Данная команда применяется на связнный узел.

Пример

В этом примере показано, как настроить подкольцо физического кольца "ring2".

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erp)#sub-ring ring1
Switch(config-erp)#
```

30-10 profile

Данная команда используется для привязки экземпляра ERPS к профилю G.8032. Используйте форму **no**, чтобы удалить привязку.

profile *PROFILE-NAME*
no profile

Параметры

PROFILE-NAME	Указывает имя профиля, которое должно быть связано с экземпляром ERP.

По умолчанию

Нет

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для привязки экземпляра ERP к профилю G.8032. Несколько экземпляров ERP могут быть связаны с одним и тем же профилем G.8032.

Пример

В этом примере показано, как связать профиль "campus" с экземпляром 1.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring1
Switch(config-erp)#instance 1
Switch(config-erp-instance)#profile campus
Switch(config-erp-instance)#
```

30-11 port0

Данная команда используется для указания первого порта физического кольца. Используйте форму **no**, чтобы удалить заданные настройки.

port0 interface *INTERFACE-ID*
no port0

Параметры

INTERFACE-ID	Укажите interface ID порта кольца. Доступны физические порты и port-channel.

По умолчанию

Нет

Режим ввода команды

ERPS Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить первый порт физического кольца.

Пример

В этом примере показано, как настроить интерфейс "eth1/0/1" в качестве первого кольцевого порта кольца G.8032 "ring1".

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring1
Switch(config-erp)#port0 interface eth1/0/1
Switch(config-erp)#
```

30-12 port1

Данная команда используется для указания второго порта физического кольца. Используйте форму **no**, чтобы удалить заданные настройки.

port1 {interface *INTERFACE-ID* **| none}**
no port1

Параметры

INTERFACE-ID	Укажите второй порт кольца. Доступны физические порты и port-channel.
none	Укажите, чтобы настроить связанный узел в качестве конеч ного локального узла подкольца.

По умолчанию

Нет

Режим ввода команды

ERPS Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить второй порт физического кольца. Используйте команду **port1 none**, чтобы настроить связанный узел в качестве конечного локального узла подкольца.

Пример

В данном примере показано, как настроить связанный узел в качестве конечного локального узла кольца G.8032 «ring2».

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erp)#port1 none
Switch(config-erp)#
```

30-13 revertive

Данная команда используется для возвращения к действующему средству передачи в случае устранения неисправности. Используйте форму **no**, чтобы продолжить использование RPL, при условии его исправности, после устранения ошибки на коммутаторе.

revertive
no revertive

Параметры

Нет

По умолчанию

По умолчанию этот параметр является **revertive**.

Режим ввода команды

G.8032 Profile Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если дефект был устранен, канал трафика вернется после истечения таймера WTR, что используется для предотвращения переключения состояний защиты, вызванных прерывистыми дефектами.

В нереверсивном режиме канал трафика продолжает использовать RPL, если он не вышел из строя после устранения состояния "дефект коммутационного канала". Поскольку при кольцевой защите Ethernet ресурсы рабочей транспортной сущности могут быть более оптимизированы, в некоторых случаях более желательно вернуться к этой рабочей транспортной сущности, как только все кольцевые каналы станут доступны. Это происходит за счет дополнительного прерывания трафика. В некоторых случаях может не быть преимущества немедленного возврата к рабочей транспортной сущности, а в некоторых случаях даже можно избежать второго прерывания трафика, не возвращаясь к переключению защиты.

Пример

В этом примере показано, как настроить кольца в профиле "campus" для работы в нереверсивном режиме.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 profile campus
Switch(config-g8032-ring-profile)#no revertive
Switch(config-g8032-ring-profile)#
```

30-14 rpl

Данная команда используется для настройки узла в качестве RPL Owner или RPL Neighbor, а также для назначения порта RPL. Используйте форму **no**, чтобы удалить настройки RPL.

rpl {port0 | port1} [owner]
no rpl

Параметры

port0	Укажите, чтобы настроить порт 0 в качестве порта RPL.
port1	Укажите, чтобы настроить порт 1 в качестве порта RPL.
owner	(Опционально) Укажите, чтобы настроить узел кольца в качестве RPL Owner для сконфигурированного экземпляра.

По умолчанию

Нет

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для настройки узла в качестве владельца RPL или соседа RPL, или для назначения порта в качестве порта RPL.

Пример

В этом примере показано, как настроить порт 0 в качестве порта RPL экземпляра ERP "1".

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring1
Switch(config-erp)#instance 1
Switch(config-erp-instance)#rpl port0
Switch(config-erp-instance)#
```

30-15 show ethernet ring g8032

Эта команда используется для отображения информации об экземплярах ERP.

show ethernet ring g8032 {status | brief}

Параметры

status	Указывает для отображения статуса экземпляров ERP.
brief	Указывает на отображение краткой информации об экземплярах ERP.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию об ERPS.

Пример

В данном примере показано, как отобразить подробную информацию об ERP.

```
Switch#show ethernet ring g8032 status

 Ethernet ring ring2,instance 0
 ---------------------------------------
     Description:
     MEL: 1
     Connect sub ring: ring1
     R-APS Channel: invalid r-aps vlan,Protected VLAN:
     Profile:
     Guard timer: 500 milliseconds
     Hold-Off timer: 0 milliseconds
     WTR timer: 5 minutes
     Revertive
     Instance State: Deactivated
     Admin RPL: -
     Operational RPL: -
     Port0 State: Forwarding
     Port1 State: Forwarding
     Admin RPL Port: -
     Operational RPL Port: -

 Ethernet ring campus,instance 0
 ---------------------------------------
     Description:
     MEL: 1
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

В этом примере показано, как отобразить краткую информацию об экземплярах ERP.

```
Switch#show ethernet ring g8032 brief

Profile                          Inst Status      Port-State
                                 .ID
-------------------------------- ---  ----------- ------------------
                                 0    Deactivated p0:-,Forwarding
                                                  p1:-,Forwarding
                                 0    Deactivated p0:-,Forwarding
                                                  p1:-,Forwarding
campus                           1    Deactivated p0:eth1/0/1,Forwarding(RPL)
                                                  p1:-,Forwarding
                                 0    Deactivated p0:-,Forwarding
                                                  p1:-,Forwarding

 Total Entries: 4

Switch#
```

Отображаемые параметры

MEL	Значение MEL кольца экземпляра ERPS.
R-APS Channel	R-APS VLAN экземпляра ERPS.
Protected VLANs	Защищенные VLAN экземпляра ERPS.
Profile	Профиль, ассоциированный с экземпляром ERPS.
Guard Timer	Значение Guard Timer профиля.
Hold-Off Timer	Значение Hold-Off Timer профиля.
WTR Timer	Значение WTR Timer профиля.
TC Propagation State	TC распространяются / не распространяются в кольце.
Revertive / Non-revertive	Реверсивный/нереверсивный режим работы колец.
Instance Status	Текущий статус узла кольца экземпляра ERPS. (Deactivated / Init / Idle / Protection / force / manual / pending).
Port0 / Port1	Текущая роль кольцевого порта. (Interface_id / virtual_channel).
RPL Port	Текущие настройки RPL. (Port0 / Port1 / None).
Ring port0/port1 state	Статус кольцевых портов экземпляра ERPS. (Forwarding / Blocking / SF / SF blocked).
RingType	Тип кольца (основное кольцо / подкольцо).
Node Type	Владелец RPL.
Status	Текущее состояние экземпляра ERP. Это может быть одно из следующих значений: **Deactivated**: Экземпляр ERP деактивирован. **Init**: Экземпляр инициализируется. **Idle**: Экземпляр находится в нормальном состоянии. Порт RPL заблокирован. **Protection** (Защита): Экземпляр обнаруживает сбой на

	каком-либо кольцевом порту. Порт RPL восстанавливается для защиты порта.
Port-State	Текущее состояние кольцевых портов. (- / Переадресован / Заблокирован)

30-16 activate

Данная команда используется для включения экземпляра ERPS. Используйте форму **no**, чтобы отключить экземпляр ERPS.

activate
no activate

Параметры

Нет

По умолчанию

По умолчанию эта опция **no activate**.

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для активации или деактивации указанного экземпляра ERP. Перед активацией экземпляра ERP необходимо настроить кольцевые порты, канал APS и профиль ERP.

Активированный экземпляр ERP будет находиться в нерабочем состоянии, если указанный канал APS не существует, или указанные порты не являются тегированными портами-членами VLAN канала APS.

Пример

В данном примере показано, как активировать экземпляр 1.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring1
Switch(config-erp)#instance 1
Switch(config-erp-instance)#activate
Switch(config-erp-instance)#
```

35-18 timer

Данная команда используется для того, чтобы настроить таймеры для профиля ERPS. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

timer {guard *MILLI-SECONDS* **| hold-off** *SECONDS* **| wtr** *MINUTES***}**
no timer [guard | hold-off | wtr]

Параметры

guard *MILLI-SECONDS*	Укажите значение Guard Timer в диапазоне от 10 до 2000 миллисекунд. Указанное значение должно быть кратным 10.
hold-off *SECONDS*	Укажите значение Hold-Off Timer в диапазоне от 0 до 10 секунд.
wtr *MINUTES*	Укажите значение WTR Timer в диапазоне от 1 до 12 минут.

По умолчанию

Значение Guard Timer по умолчанию – 500 миллисекунд.
Значение Hold-Off Timer по умолчанию – 0.
Значение WTR Timer по умолчанию – 5 минут.

Режим ввода команды

G.8032 Profile Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для настройки таймеров для домена ERP.

Пример

В этом примере показано, как настроить таймер охраны на 700 для профиля campus.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 profile campus
Switch(config-g8032-ring-profile)#timer guard 700
Switch(config-g8032-ring-profile)#
```

31. Команды File System

31-1 cd

Данная команда используется для смены текущего каталога.

cd [*DIRECTORY-URL***]**

Параметры

DIRECTORY-URL	(Опционально) Укажите путь к каталогу. Если путь не указан, будет отображен текущий каталог.

По умолчанию

По умолчанию текущим каталогом является корневой каталог в файловой системе внутренней памяти.

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Если путь не указан, текущий каталог не будет сменен.

Пример

В данном примере показано, как изменить текущий каталог на каталог "log" в файловой системе "c:/".

```
Switch# dir

Directory of /c:
1 d             0 Dec 29 2013 17:49:36  images
2 d             0 Jan 02 2013 18:42:53  configurations
3 d             0 Jan 02 2013 18:42:53  log
4 -           639 Jan 03 2013 12:09:32  new_config.cfg

20578304 bytes total (3104544 bytes free)

Switch#cd c:/log
Switch#dir

Directory of /c:/log
No files in directory
20578304 bytes total (3104544 bytes free)

Switch#
```

В данном примере показано, как отобразить текущий каталог.

```
Switch# cd

Current directory is /c:/log

Switch#
```

31-2 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Файл программного обеспечения или файл конфигурации, указанный в качестве загрузочного файла, удалить невозможно.

Пример

В данном примере показано, как удалить файл «test.txt» из файловой системы внутренней памяти.

```
Switch# delete c:/test.txt

Delete test.txt? (y/n) [n] y
File is deleted

Switch#
```

31-3 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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 /
1 d--            0 Jun 31 2013 17:49:36  c:
2 d--            0 Jun 31 2013 18:42:53  d:
0 bytes total (0 bytes free)

Switch#
```

31-4 mkdir

Данная команда используется для создания каталога в текущем каталоге.

mkdir *DIRECTORY-NAME*

Параметры

DIRECTORY-NAME	Укажите имя каталога.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы создать каталог в текущем каталоге.

Пример

В данном примере показано, как создать каталог «newdir» в текущем каталоге.

```
Switch# mkdir newdir
Switch#
```

31-5 more

Данная команда используется для отображения содержимого файла.

more *FILE-URL*

Параметры

FILE-URL	Укажите путь к файлу, который необходимо отобразить.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы отобразить содержимое файла в файловой системе. Обычно команда применяется для отображения текстовых файлов. Нестандартные печатные символы будут отображены как нечитаемые знаки или пробелы.

Пример

В данном примере показано, как отобразить содержимое файла «usr_def.conf».

```
Switch# more  /c:/configuration/usr_def.conf

!DGS-1510
!Firmware Version:1.70.005
!Slot      Model
!------ ------------------
! 1        DGS-1510-28XMP
! 2        -
! 3        DGS-1510-28XMP
! 4        DGS-1510-28XMP
!
ip igmp snooping vlan 1
!.
end

Switch#
```

31-6 rename

Данная команда используется для переименования файла.

rename *FILE-URL1 FILE-URL2*

Параметры

FILE-URL1	Укажите путь к файлу, который необходимо переименовать.
FILE-URL2	Укажите путь к переименованному файлу.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Переименованный файл может располагаться в том же или другом каталоге.

Пример

В данном примере показано, как изменить имя файла с «doc.1» на «test.txt».

```
Switch# rename /c:/doc.1 /c:/test.txt

Rename file doc.1 to text.txt? (y/n) [n] y

Switch#
```

31-7 rmdir

Данная команда используется для удаления каталога из файловой системы.

rmdir *DIRECTORY-NAME*

Параметры

DIRECTORY-NAME	Укажите имя каталога, который необходимо удалить.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы удалить каталог из текущего каталога.

Пример

В данном примере показано, как удалить каталог «newdir» из текущего каталога.

```
Switch# rmdir newdir

Remove directory newdir? (y/n) [n] y
The directory is removed

Switch#
```

31-8 show storage media-info

Данная команда используется для отображения информации о накопителе.

show storage media-info [unit *UNIT-ID***]**

Параметры

unit *UNIT-ID*	(Опционально) Укажите Unit ID устройства в стеке. Если Unit ID не указан, будут отображены все устройства.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию о доступных накопителях системы.

Пример

В данном примере показано, как отобразить информацию о доступных накопителях на всех устройствах стека.

```
Switch# show storage media-info

Unit  Drive  Media-Type  Size     FS-Type   Label
----  -----  ----------  -------  --------  -------------
 1    c:     FLASH       31M      FFS
 2    c:     FLASH       31M      FFS
 2    d:     SD Card     256M     FAT32     test
 3    c:     FLASH       31M      FFS

Switch#
```

32. Команды Filter Database (FDB)

32-1 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

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#
```

32-2 mac-address-table aging-time

Данная команда используется для настройки времени устаревания MAC-адресов в таблице. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Укажите время устаревания 0, чтобы отключить функцию устаревания MAC-адресов в таблице.

Пример

В данном примере показано, как установить значение времени устаревания на 200 секунд.

```
Switch# configure terminal
Switch(config)# mac-address-table aging-time 200
Switch(config)#
```

32-3 mac-address-table aging destination-hit

Данная команда используется для включения функции Destination MAC Address Triggered Update. Используйте форму **no**, чтобы отключить данную функцию.

mac-address-table aging destination-hit
no mac-address-table aging destination-hit

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Функция source MAC Address Triggered Update всегда включена. Hit Bit записей MAC-адреса, соответствующего порту, получающему пакет, будет обновлен на основании MAC-адреса источника (source) и VLAN пакета. Если пользователь включает функцию Destination MAC Address Triggered Update при помощи команды **mac-address-table aging destination-hit**, Hit Bit записей MAC-адреса, соответствующего порту, передающему пакет, будет обновлен на основании MAC-адреса назначения (destination) и VLAN пакета.

Функция Destination MAC Address Triggered Update увеличивает частоту обновления Hit Bit записей MAC-адреса и уменьшает лавинное распространение трафика при помощи времени устаревания записей MAC-адреса.

Пример

В данном примере показано, как включить функцию Destination MAC Address Triggered Update.

```
Switch# configure terminal
Switch(config)# mac-address-table aging destination-hit
Switch(config)#
```

32-4 mac-address-table learning

Данная команда используется для включения изучения MAC-адресов на физическом порту или VLAN. Используйте форму **no**, чтобы отключить данную функцию.

mac-address-table learning interface {*INTERFACE-ID* **[, | -]}**
no mac-address-table learning interface {vlan *VLAN-ID* **[, | -] |** *INTERFACE-ID* **[, | -]}**

Параметры

INTERFACE-ID	Укажите интерфейс физического порта, 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для включения или отключения обучения 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 ethernet 1/0/5
Switch(config)#
```

32-5 mac-address-table notification change

Данная команда используется для включения/настройки функции уведомлений о MAC-адресах. Используйте форму **no**, чтобы отключить функцию или вернуться к настройкам по умолчанию.

mac-address-table notification change [interval *SECONDS* **| history-size** *VALUE***]**
no mac-address-table notification change [interval | history-size]

Параметры

interval *SECONDS*	(Опционально) Укажите интервал отправки трап-сообщений о MAC-адресах в диапазоне от 1 до 2147483647 секунд. Значение по умолчанию – 1 секунда.
history-size *VALUE*	(Опционально) Укажите максимальное количество записей втаблице истории уведомлений. Доступный диапазон значений: от 0 до 500 записей. Значение по умолчанию – 1 запись.

По умолчанию

Уведомление о MAC-адресе отключено.
Интервал ловушек по умолчанию составляет 1 секунду.
Количество записей в таблице истории по умолчанию равно 1.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 трапы. 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)#
```

32-6 mac-address-table static

Данная команда используется для добавления статического адреса в таблицу MAC-адресов. Используйте форму **no**, чтобы удалить запись из таблицы.

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

Уровень команды по умолчанию

Уровень 12

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 этом примере показано, как добавить статический адрес C2:F3:22:0A:12:F4 в таблицу MAC-адресов. Он также указывает, что при получении любого пакета в сети VLAN 4, имеющего MAC-адрес назначения C2:F3:22:0A:12:F4, он будет перенаправлен на порт 1.

```
Switch# configure terminal
Switch(config)# mac-address-table static C2:F3:22:0A:12:F4 vlan 4 interface
eth1/0/1
Switch(config)#
```

В этом примере показано, как добавить статический адрес C2:F3:22:0A:22:33 в таблицу MAC-адресов. Он также указывает, что при получении любого пакета в сети VLAN 4, имеющего MAC-адрес назначения C2:F3:22:0A:22:33, он будет перенаправлен на порт-канал 2.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/5-6
Switch(config-if-range)# channel-group 2 mode on
Switch(config-if-range)# exit
Switch(config)# mac-address-table static C2:F3:22:0A:22:33 vlan 4 interface port-
channel 2
Switch(config)#
```

37-7 multicast filtering-mode

Данная команда используется для настройки способа обработки групповых пакетов на интерфейсе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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 основани 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

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

32-8 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

При указании параметра **interface** будет отображена индивидуальная запись, чей интерфейс передачи соответствует указанному интерфейсу.

Пример

В этом 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#
```

32-9 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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#
```

32-10 show mac-address-table learning

Данная команда используется для отображения статуса изучения MAC-адресов.

show mac-address-table learning interface [*INTERFACE-ID* **[, | -]]**

Параметры

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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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 ethernet 1/0/1-10

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#
```

32-11 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Если параметр не указан, будет отображена глобальная конфигурация. Используйте параметр **interface** для отображения информации обо всех интерфейсах. Используйте параметр **interface** *INTERFACE-ID* для отображения информации об указанном интерфейсе.

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: Disabled
Interval between Notification Traps: 1 seconds
Maximum Number of Entries Configured in History Table: 1
Current History Table Length: 0
MAC Notification Trap State: Disabled

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#
```

32-12 show multicast filtering-mode

Данная команда используется для отображения режима фильтрации при обработке групповых пакетов, полученных на интерфейсе.

show multicast filtering-mode [interface *INTERFACE-ID***]**

Параметры

interface *INTERFACE-ID*	(Опционально) Укажите VLAN, которую необходимо отобразить.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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#
```

32-13 snmp-server enable traps mac-notification change

Данная команда используется для включения отправки SNMP Trap об уведомлениях MAC. Используйте форму **no**, чтобы отключить данную функцию.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить 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)#
```

32-14 snmp trap mac-notification change

Данная команда используется для включения уведомлений об изменении MAC-адреса на указанном интерфейсе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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 отправка трапов о добавлении/удалении адреса отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 интерфейсеEthernet 1/0/2.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# snmp trap mac-notification change added
Switch(config-if)#
```

33. Команды GARP VLAN Registration Protocol (GVRP)

33-1 clear gvrp statistics

Данная команда используется для удаления статистики GVRP на порту.

clear gvrp statistics {all | interface *INTERFACE-ID* **[, | -]}**

Параметры

all	Укажите, чтобы обнулить счетчики статистики GVRP, ассоциированные со всеми интерфейсами.
interface *INTERFACE-ID*	Укажите интерфейсы, которые 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

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы обнулить счетчики GVRP.

Пример

В данном примере показано, как удалить статистику для всех интерфейсов.

```
Switch# clear gvrp statistics all
Switch#
```

33-2 gvrp global

Данная команда используется для глобального включения функции GVRP. Используйте форму **no**, чтобы глобально отключить функцию GVRP.

gvrp global
no gvrp global

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

GVRP можно включить как глобально, так и на отдельном порту.

Пример

В данном примере показано, как включить GVRP-протокол глобально.

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

33-3 gvrp enable

Данная команда используется для включения функции GVRP на порту. Используйте форму **no**, чтобы отключить данную функцию.

gvrp enable
no gvrp enable

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда доступна как для физических портов, так и для конфигурации интерфейса порт-канала. Эта команда действует только для Hybrid mode и mode Trunk.

Пример

В данном примере показано, как включить функцию GVRP на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# gvrp enable
Switch(config-if)#
```

33-4 gvrp advertise

Используйте данную команду, чтобы указать VLAN, для которых разрешено анонсирование припомощи GVRP-протокола. Используйте форму **no**, чтобы отключить данную функцию.

gvrp advertise {all | [add | remove] *VLAN-ID* **[, | -]}**
no gvrp advertise

Параметры

all	Укажите, чтобы включить анонсирование для всех VLAN на интерфейсе.
add	(Опционально) Укажите одну или несколько VLAN, которые необходимо добавить в список анонсирования.
remove	(Опционально) Укажите одну или несколько VLAN, которые необходимо удалить из списка анонсирования.
VLAN-ID	Укажите VLAN ID, который необходимо добавить в список анонсирования или удалить из данного списка. Если не указан параметр **add** или **remove**, список указанных VLAN заменит текущий список анонсирования. Доступный 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

По умолчанию анонсирование VLAN отключено.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки физических портов и port-channel в режимах Hybrid Mode и Trunk Mode. Используйте команду **gvrp advertise**, чтобы включить функцию анонсирования GVRP для указанных VLAN на указанном интерфейсе. Предварительно необходимо включить GVRP.

Пример

В данном примере показано, как включить функцию анонсирования для VLAN 1000 на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# gvrp advertise 1000
Switch(config-if)#
```

33-5 gvrp vlan create

Данная команда используется для того, чтобы включить создание Dynamic VLAN. Используйте форму **no**, чтобы отключить данную функцию.

gvrp vlan create
no gvrp vlan create

Параметры

Нет

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если данная функция включена и на порту обнаружено новое членство VLAN, но при этом данной VLAN не существует, VLAN будет создана автоматически. Иначе изученная VLAN не будет создана.

Пример

В данном примере показано, как включить создание dynamic VLAN, зарегистрированных с помощью GVRP-протокола.

```
Switch# configure terminal
Switch(config)# gvrp vlan create
Switch(config)#
```

33-6 gvrp forbidden

Данная команда используется для указания порта, которому запрещено быть членом обозначенной VLAN. Используйте форму **no**, чтобы удалить статус запрещенного члена всех VLAN для порта.

gvrp forbidden {all | [add | remove] *VLAN-ID* **[, | -]}**
no gvrp forbidden

Параметры

all	Укажите, чтобы запретить на интерфейсе все VLAN, кроме VLAN 1.
add	(Опционально) Укажите одну или несколько VLAN, которые необходимо добавить в список запрещенных VLAN.
remove	(Опционально) Укажите одну или несколько VLAN, которые необходимо удалить из списка запрещенных VLAN.
VLAN-ID	Укажите список запрещенных VLAN. Если не указан параметр **add** или **remove**, список данных VLAN заменит текущий список запрещенных VLAN. Доступный диапазон значений: от 2 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

По умолчанию ни одна из VLAN не запрещена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки физических портов и port-channel в режимах Hybrid Mode иTrunk Mode. Порт, указанный в качестве запрещенного порта VLAN, не может стать членом VLAN при помощи GVRP. VLAN, обозначенная при помощи данной команды, может не существовать.

Команда влияет только на работу GVRP, при этом GVRP необходимо предварительно включить.

Пример

В данном примере показано, как настроить порт ethernet 1/0/1 в качестве запрещенного порта для VLAN 1000 при помощи GVRP.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# gvrp forbidden 1000
Switch(config-if)#
```

33-7 gvrp timer

Данная команда используется для настройки значения таймера GVRP на порту. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

gvrp timer [join *TIMER-VALUE*] **[leave** *TIMER-VALUE*] **[leave-all** *TIMER-VALUE*]
no gvrp timer [join] [leave] [leave-all]

Параметры

join	(Опционально) Установите значение таймера для входа в группу. Единицы измерения – сотые доли секунды.
leave	(Опционально) Установите значение таймера для выхода из группы. Единицы измерения – сотые доли секунды.
leave-all	(Опционально) Установите значение таймера для выхода из всех групп. Единицы измерения – сотые доли секунды.
TIMER-VALUE	(Опционально) Установите значение таймера. Доступный диапазон значений: от 10 до 10000 сотых долей секунды.

По умолчанию

Join: 20
Leave: 60
Leave-all: 1000

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить значение таймера GVRP на порту.

Пример

В данном примере показано, как настроить значение таймера для выхода из всех групп на порту Ethernet 1/0/1. Установленное значение – 500 сотых долей секунды.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# gvrp timer leave-all 500
Switch(config-if)#
```

33-8 show gvrp configuration

Данная команда используется для отображения настроек GVRP.

show gvrp configuration [interface [*INTERFACE-ID* **[, | -]]]**

Параметры

interface	(Опционально) Укажите, чтобы отобразить настройки GVRP для интерфейса. Если interface ID не указан, будут отображены настройки всех интерфейсов.
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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить настройки GVRP. Если не указан ни один из параметров, будут отображены глобальные настройки GVRP.

Пример

В данном примере показано, как отобразить глобальные настройки GVRP.

```
Switch# show gvrp configuration

Global GVRP State      : Enabled
Dynamic VLAN Creation : Disabled

Switch#
```

В этом примере показано, как отобразить конфигурацию GVRP на интерфейсах eh3/0/5 - eth3/06.

```
Switch# show gvrp configuration interface eth3/0/5-3/0/6

eth3/0/5
GVRP Status     : Enabled
Join Time       : 20 centiseconds
Leave Time      : 60 centiseconds
Leave-All Time  : 1000 centiseconds
Advertise VLAN  : 1-4094
Forbidden VLAN  : 3-5

eth3/0/6
GVRP Status     : Enabled
Join Time       : 20 centiseconds
Leave Time      : 60 centiseconds
Leave-All Time  : 1000 centiseconds
Advertise VLAN  : 1-3
Forbidden VLAN  : 5-8

Switch#
```

33-10 show gvrp statistics

Данная команда используется для отображения статистики GVRP на порту.

show gvrp statistics [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

User EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить порты, на которых включен режим GVRP.

Пример

В этом примере показано, как отобразить статистику для GVRP интерфейсов eth3/0/5 - eth3/0/6.

```
Switch# show gvrp statistics interface eth3/0/5-3/0/6

Port        JoinEmpty       JoinIn  LeaveEmpty     LeaveIn   LeaveAll    Empty
----------- ----------- ---------- ----------- ---------- ---------- --------
eth3/0/5 RX          0          0           0          0          0          0
         TX 4294967296 4294967296  4294967296 4294967296 4294967296 4294967296
eth3/0/6 RX          0          0           0          0          0          0
         TX          0          0           0          0          0          0

Switch#
```

34. Команды Gratuitous ARP

34-1 ip arp gratuitous

Данная команда используется для включения изучения пакетов Gratuitous ARP в таблице ARP-кэша. Используйте форму **no**, чтобы отключить ARP control.

ip arp gratuitous
no ip arp gratuitous

Параметры

Нет

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

34-2 ip gratuitous-arps

Данная команда используется для того, чтобы включить передачу пакетов Gratuitous ARP Request. Испольуйте форму **no**, чтобы отключить передачу.

ip gratuitous-arps [dad-reply]
no ip gratuitous-arps [dad-reply]

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

34-3 arp gratuitous-send interval

Данная команда используется для установки интервала отправки сообщений Gratuitous ARP Request на интерфейсе. Используйте форму **no**, чтобы отключить данную функцию.

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

Уровень команды по умолчанию

Уровень 12

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 vlan 100
Switch(config-if)# arp gratuitous-send interval 1
Switch(config-if)#
```

34-4 snmp-server enable traps gratuitous-arp

Данная команда используется для включения отправки SNMP-уведомлений об обнаружении дублированного IP-адреса Gratuitous ARP. Используйте форму **no**, чтобы отключить данную функцию.

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

Уровень команды по умолчанию

Уровень 12

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)#
```

35. Команды управления интерфейсом

35-1 clear counters

Данная команда используется для сброса всех счетчиков для указанных интерфейсов.

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

Параметры

all	Укажите, если необходимо сбросить счетчики для всех интерфейсов.
interface *INTERFACE-ID*	Укажите настраиваемые интерфейсы. Интерфейсами могут считаться физические порты, порт управления OOB, port-channel или интерфейсы VLAN 2-го уровня.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для сброса счетчиков для интерфейса физического порта.

Пример

В данном примере показан процесс сброса счетчиков для Ethernet 1/0/1.

```
Switch# clear counters interface ethernet 1/0/1
Switch#
```

35-2 description

Данная команда используется для добавления описания для интерфейса. При использовании формы **no** команда удалит описание.

description *STRING*
no description

Параметры

STRING	Описание для интерфейса. Максимально допустимое количество символов – 64.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Описание может быть добавлено к любому предварительно определенному типу интерфейса, но не к динамически создаваемым интерфейсам, таким как динамические VLAN, создаваемые GVRP. Указанное описание соответствует объекту MIB "ifAlias", определенному в RFC 2233.

Пример

В данном примере показано, как добавить описание "Physical Port 10" к порту 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" к интерфейсу виртуальной локальной сети уровня 2.

```
Switch#configure terminal
Switch(config)#interface l2vlan 1
Switch(config-if)#description Data VLAN
Switch(config-if)#
```

35-3 interface

Данная команда используется для входа в режим Interface Configuration Mode для одного интерфейса. При использовании формы **no** команда удалит интерфейс.

interface *INTERFACE-ID*
no interface *INTERFACE-ID*

Параметры

INTERFACE-ID	Указывает идентификатор интерфейса. Идентификатор

	интерфейса формируется из типа интерфейса и номера интерфейса. Типы интерфейсов следующие: - Ethernet - порт коммутатора Ethernet со всеми различными носителями. - Vlan - интерфейс VLAN. - Port-channel - интерфейс агрегированного портового канала. - range - Вход в режим конфигурации диапазона интерфейсов для нескольких интерфейсов. - L2vlan - интерфейс виртуальной локальной сети второго уровня IEEE 802.1Q.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда входит в режим конфигурации интерфейса для конкретного интерфейса. Формат номера интерфейса зависит от типа интерфейса. Для интерфейсов физического порта 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 интерфейсов уровня 3. Используйте команду vlan в режиме глобальной конфигурации для создания сети VLAN перед созданием интерфейсов уровня 3. Используйте команду no interface vlan для удаления интерфейса 3-го уровня.

Интерфейс канала порта автоматически создается, когда для интерфейса физического порта настроена команда **channel-group**. Интерфейс портового канала автоматически удаляется, если для интерфейса физического порта не настроена команда **channel-group**. Для удаления порт-канала используйте команду **no interface port- channel**.

Интерфейс **L2vlan** используется только для добавления описаний к существующим L2 VLAN. Команда **interface l2vlan** не создает нового интерфейса, равно как и команда no не удаляет существующий интерфейс.

Пример

В данном примере показано, как войти в режим Interface Configuration Mode для Ethernet 1/0/5.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/5
Switch(config-if)#
```

В данном примере показано, как войти в режим Interface Configuration Mode для VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan 100
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)#
```

35-4 interface range

Данная команда используется для входа в режим Interface Range Configuration Mode для нескольких интерфейсов.

interface range *INTERFACE-ID* **[, | -]**

Параметры

INTERFACE-ID	Указывает идентификатор интерфейса. Идентификатор интерфейса формируется из типа интерфейса и номера интерфейса. Типы интерфейсов следующие следующие: - Ethernet - порт коммутатора Ethernet со всеми различными носителями. - L2vlan - интерфейс IEEE 802.1Q Layer 2 Virtual LAN.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для входа в режим Interface Configuration Mode для указанного диапазона интерфейсов. Команды, введенные в режиме Interface Range Mode, применяются ко всем интерфейсам в диапазоне.

Пример

В данном примере показано, как войти в режим конфигурации диапазона интерфейсов для портов 1-5 и порта 8.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/1-5,1/0/8
Switch(config-if-range)#
```

35-5 show counters

Данная команда используется для отображения информации об интерфейсе.

show counters [interface *INTERFACE-ID***]**

Параметры

interface *INTERFACE-ID*	(Опционально) Укажите необходимый интерфейс: физический порт, port-channel или VLAN. Если интерфейс не указан, будут отображаться счетчики для всех интерфейсов.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения статистики счетчиков для интерфейса.

Пример

В этом примере показано, как отобразить счетчики на порту 1.

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

eth1/0/1 counters
rxHCTotalPkts                    : 1176
txHCTotalPkts                    : 348
rxHCUnicastPkts                  : 0
txHCUnicastPkts                  : 0
rxHCMulticastPkts                : 755
txHCMulticastPkts                : 0
rxHCBroadcastPkts                : 421
txHCBroadcastPkts                : 348
rxHCOctets                       : 112581
txHCOctets                       : 126324
rxHCPkt64Octets                  : 21
rxHCPkt65to127Octets             : 982
rxHCPkt128to255Octets            : 173
rxHCPkt256to511Octets            : 0
rxHCPkt512to1023Octets           : 0
rxHCPkt1024to1518Octets          : 0
rxHCPkt1519to1522Octets          : 0
rxHCPkt1519to2047Octets          : 0
rxHCPkt2048to4095Octets          : 0
rxHCPkt4096to9216Octets          : 0
txHCPkt64Octets                  : 0
txHCPkt65to127Octets             : 0
txHCPkt128to255Octets            : 0
txHCPkt256to511Octets            : 348
txHCPkt512to1023Octets           : 0
txHCPkt1024to1518Octets          : 0
txHCPkt1519to1522Octets          : 0
txHCPkt1519to2047Octets          : 0
txHCPkt2048to4095Octets          : 0
txHCPkt4096to9216Octets          : 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
rxStormAndFDBDropPkts            : 0
rxMTUDropPkts                    : 0

txCollisions                     : 0
ifInErrors                       : 0
ifOutErrors                      : 0
ifInDiscards                     : 1175
ifInUnknownProtos                : 0
```

```
ifOutDiscards                    : 0
txDelayExceededDiscards          : 0
txCRC                            : 0
txSTPDropPkts                    : 0
txHOLDropPkts                    : 0

dot3StatsAligrmentErrors         : 0
dot3StatsFCSErrors               : 0
dot3StatsSingleColFrames         : 0
dot3StatsMultiColFrames          : 0
dot3StatsSQETestErrors           : 0
dot3StatsDeferredTransmissions   : 0
dot3StatsLateCollisions          : 0
dot3StatsExcessiveCollisions     : 0
dot3StatsInternalMacTransmitErrors : 0
dot3StatsCarrierSenseErrors      : 0
dot3StatsFrameTooLongs           : 0
dot3StatsInternalMacReceiveErrors : 0

linkChange                       : 1

Switch#
```

Отображаемые параметры

rxHCTotalPkts	Счетчик принятых пакетов. Возрастает с каждым принятым пакетом (включая поврежденные пакеты, все одноадресные, широковещательные и многоадресные пакеты и пакеты управления MAC).
txHCTotalPkts	Счетчик переданных пакетов. Возрастает с каждым переданным пакетом (включая поврежденные пакеты, все одноадресные, широковещательные и многоадресные пакеты и пакеты управления MAC).
rxHCUnicastPkts	Счетчик принятых пакетов одноадресной рассылки. Возрастает с каждым успешно принятым пакетом одноадресной рассылки.
txHCUnicastPkts	Счетчик переданных пакетов одноадресной рассылки. Возрастает с каждым успешно переданным пакетом одноадресной рассылки.
rxHCMulticastPkts	Счетчик принятых пакетов многоадресной рассылки. Возрастает с каждым успешно принятым пакетом многоадресной рассылки, исключая пакеты управления MAC.
txHCMulticastPkts	Счетчик переданных пакетов многоадресной рассылки. Возрастает с каждым успешно переданным пакетом многоадресной рассылки, исключая пакеты управления MAC.
rxHCBroadcastPkts	Счетчик принятых пакетов широковещательной рассылки. Возрастает с каждым успешно принятым пакетом широковещательной рассылки.
txHCBroadcastPkts	Счетчик переданных пакетов широковещательной

	рассылки. Возрастает с каждым успешно переданным пакетом широковещательной рассылки.
rxHCOctets	Счетчик принятых байтов. Возрастает с подсчетом байтов принятых пакетов, исключая поврежденные пакеты. (Исключаябиты кадров, но включая байты FCS) **Примечание**: Для усеченного пакета счетчик учитывает толькоразмер max-rcv-frame.
txHCOctets	Счетчик переданных байтов. Возрастает с подсчетом байтов переданных пакетов, исключая поврежденные пакеты. (Исключая биты кадров, но включая байты FCS)
rxHCPkt64Octets	Счетчик принятых 64-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), до 64 байт включительно (исключая биты кадров, но включая байты FCS).
rxHCPkt65to127Octets	Счетчик принятых 64 – 127-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 65 до 127 байт включительно (исключая биты кадров, но включая байты FCS).
rxHCPkt128to255Octets	Счетчик принятых 128 – 255-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 128 до 255 байт включительно (исключая биты кадров, но включая байты FCS).
rxHCPkt256to511Octets	Счетчик принятых 256 – 511-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 256 до 511 байт включительно (исключая биты кадров, но включая байты FCS).
rxHCPkt512to1023Octets	Счетчик принятых 512 – 1023-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 512 до 1023 байт включительно (исключая биты кадров, но включая байты FCS).
rxHCPkt1024to1518Octets	Счетчик принятых 1024 – 1518-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 1024 до 1518 байтвключительно (исключая биты кадров, но включая байты FCS).
rxHCPkt1519to1522Octets	Счетчик принятых допустимых 1519 – 1522-байтовых кадров VLAN. Возрастает с каждым допустимым принятым кадром VLAN (исключая FCS, Symbol, ошибка Truncated), от 1519 до1522 байт включительно (исключая биты кадров, но включая байты FCS). Подсчитываются как одиночные, так и дваждытегированные кадры.
rxHCPkt1519to2047Octets	Счетчик принятых 1519 – 2047-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 1519 до 2047 байтвключительно (исключая биты кадров, но включая

	байты FCS).
rxHCPkt2048to4095Octets	Счетчик принятых 2048 – 4095-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 2048 до 4095 байтвключительно (исключая биты кадров, но включая байты FCS).
rxHCPkt4096to9216Octets	Счетчик принятых 4096 – 9216-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 4096 до 9216 байтвключительно (исключая биты кадров, но включая байты FCS).
rxHCPkt9217to16383Octets	Счетчик принятых 9217 – 16383-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 9217 до 16383 байтвключительно (исключая биты кадров, но включая байты FCS).
txHCPkt64Octets	Счетчик переданных 64-байтовых кадров. Возрастает с каждымдопустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), до 64 байт включительно (исключая биты кадров, но включая байты FCS).
txHCPkt65to127Octets	Счетчик переданных 65 – 127-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 65 до 127 байт включительно (исключая биты кадров, но включая байты FCS).
txHCPkt128to255Octets	Счетчик переданных 128 – 255-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 128 до 255 байт включительно (исключая биты кадров, но включая байты FCS).
txHCPkt256to511Octets	Счетчик переданных 256 – 511-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 256 до 511 байт включительно (исключая биты кадров, но включая байты FCS).
txHCPkt512to1023Octets	Счетчик переданных 512 – 1023-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 512 до 1023 байт включительно (исключая биты кадров, но включая байты FCS).
txHCPkt1024to1518Octets	Счетчик переданных 1024 – 1518-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 1024 до 1518 байтвключительно (исключая биты кадров, но включая байты FCS).
txHCPkt1519to1522Octets	Счетчик переданных допустимых 1519 – 1522-байтовых кадров VLAN. Возрастает с каждым допустимым кадром VLAN (исключая FCS, Symbol, ошибку TX), от 1519 до 1522 байт включительно (исключая биты кадров, но включая байты FCS).
txHCPkt1519to2047Octets	Счетчик переданных 1519 – 2047-байтовых кадров.

	Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 1519 до 2047 байтвключительно (исключая биты кадров, но включая байты FCS).
txHCPkt2048to4095Octets	Счетчик переданных 2048 – 4095-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 2048 до 4095 байтвключительно (исключая биты кадров, но включая байты FCS).
txHCPkt4096to9216Octets	Счетчик переданных 4096 – 9216-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 4096 до 9216 байтвключительно (исключая биты кадров, но включая байты FCS).
txHCPkt9217to16383Octets	Счетчик переданных 9217 – 16383-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 9217 до 16383 байтвключительно (исключая биты кадров, но включая байты FCS).
rxCRCAlignErrors	Счетчик принятых кадров с ошибкой выравнивания. Возрастает с каждым принятым пакетом от 64 до max-rcv-frame-size (или max-rcv-frame-size+4 для тегированных кадров) октетов в длину (исключая биты кадра, но включая октеты FCS), но имеющим либо поврежденный FCS с целым числом октетов (ошибка FCS),либо поврежденный FCS с не целым числом октетов (Ошибка выравнивания).
rxUndersizedPkts	Счетчик принятых кадров неполного размера. Возрастает с каждым принятым пакетом меньше 64 байт в длину (исключая биты кадров, но включая октеты FCS), но в остальном сформированным верно (содержащим допустимый FCS).
rxFragmentPkts	Счетчик принятых фрагментов. Возрастает с каждым принятым пакетом меньше 64 байт в длину (исключая биты кадров, но включая октеты FCS), но имеющим либо поврежденный FCS с целым числом октетов (ошибка FCS), либо поврежденный FCS с не целым числом октетов (Ошибка выравнивания).
rxSymbolErrors	Счетчик принятых кадров с ошибкой кода. Возрастает с каждым принятым кадром, содержащим недопустимый символ данных, но допустимый носитель.
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 дальнейшую передачу протоколу на уровень выше. Счетчик является суммой dot3StatsAlignmentErrors, dot3StatsFCSErrors, dot3StatsFrameTooLongs и dot3StatsInternalReceiveError.
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 дальнейшем 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.
txDelayExceededDiscards	Счетчик просроченных переданных пакетов. Возрастает при передаче пакетов, которые были отброшены из-за превышениявремени передачи.
txCRC	Счетчик переданных пакетов с ошибкой FCS. Возрастает с каждым переданным пакетом, не прошедшим проверку FCS.
dot3StatsSingleColFrames	Счетчик переданных кадров с одиночной коллизией. Доступен только для режима 10/100. Возрастает с каждым переданнымкадром, испытавшим одну коллизию по время передачи.
dot3StatsMultiColFrames	Счетчик переданных кадров многочисленных коллизий. Доступен только в режиме 10/100. Возрастает с каждым успешно переданным кадром, испытавшим больше одной коллизии по время передачи.
dot3StatsDeferredTransmisions	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 вдальнейшем не подвергся коллизии во время последующей передачи.
dot3StatsLateCollisions	Счетчик кадров поздней коллизии. Доступен только в режиме 10/100. Возрастает с каждым переданным кадром с позднейколлизией во время попытки передачи.
dot3StatsExcessiveCollisions	Счетчик переданных кадров с избытком коллизий. Доступен только в режиме 10/100. Возрастает с каждым кадром, передачакоторого 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 никаким из следующих счетчиков: dot3StatsLateCollisions, dot3StatsExcessiveCollisions и dot3StatsCarrierSenseErrors.
dot3StatsFrameTooLongs	Счетчик принятых кадров слишком большой длины. Возрастает с каждым принятым кадром, превышающим размер max-rcv-frame-size.
dot3StatsInternalMacReceiveErrors	Счетчик внутренних MAC-ошибок приема. Увеличивается для кадров, для которых прием не удался из-за внутренней ошибки приема на подуровне MAC. Кадр учитывается,

	только если он не учитывается соответствующим экземпляром любого из dot3StatsFrameTooLongs, dot3StatsAlignmentErrors или dot3StatsFCSErrors.

35-6 show interfaces

Данная команда используется для просмотра информации об интерфейсе.

show interfaces [*INTERFACE-ID* **[, | -]]**

Параметры

INTERFACE-ID	(Опционально) Укажите физический порт, VLAN, интерфейс loopback или другой интерфейс.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Если интерфейс не указан, отображаться будут данные для всех интерфейсов.

Пример

В данном примере показано, как включить отображение информации об интерфейсе VLAN для интерфейса VLAN 1.

```
Switch# show interfaces vlan1

VLAN1 is enabled, link status is down
Interface type: VLAN
Interface description: VLAN 1 for MIS
MAC address: 08-00-01-22-00-00

Switch#
```

В этом примере показано, как отобразить информацию об интерфейсе для порта 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#
```

35-7 show interfaces counters

Данная команда используется для отображения счетчиков на определенных интерфейсах.

show interfaces [*INTERFACE-ID* **[, | -]] counters [errors]**

Параметры

INTERFACE-ID	(Опционально) Укажите, является ли интерфейс физическим портом или интерфейсом VLAN. Если интерфейс не указан, отображаться будут счетчики для всех интерфейсов.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
errors	(Опционально) Укажите для отображения счетчика ошибок.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения общих счетчиков, счетчиков ошибок или архивной информации для указанного или всех интерфейсов.

Пример

В этом примере показано, как отобразить счетчики портов коммутатора на портах с 1 по 8.

```
Switch#show interfaces ethernet 1/0/1-8 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 этом примере показано, как отобразить счетчики ошибок портов коммутатора.

```
Switch# show interfaces ethernet 1/0/1-8 counters errors

Port      Align-Err   Fcs-Err  Rcv-Err   Undersize  Xmit-Err  OutDiscard
--------- ---------- --------- --------  ---------- --------- -----------
eth1/0/1           0         0         0          0         0           0
eth1/0/2           0         0         0          0         0           0
eth1/0/3           0         0         0          0         0           0
eth1/0/4           0         0         0          0         0           0
eth1/0/5           0         0         0          0         0           0
eth1/0/6           0         0         0          0         0           0
eth1/0/7           0         0         0          0         0           0
eth1/0/8           0         0         0          0         0           0

Port          Single-Col Multi-Col  Late-Col    Excess-Col Carri-Sen  Runts
------------- ---------- ---------- ----------  ---------- ---------- ----------

eth1/0/1      0          0          0           0          0          0         0
eth1/0/2      0          0          0           0          0          0         0
eth1/0/3      0          0          0           0          0          0         0
eth1/0/4      0          0          0           0          0          0         0
eth1/0/5      0          0          0           0          0          0         0
eth1/0/6      0          0          0           0          0          0         0
eth1/0/7      0          0          0           0          0          0         0
eth1/0/8      0          0          0           0          0          0         0

Port          Giants     Symbol-Err SQETest-Err DeferredTx IntMacTx   IntMacRx
------------- ---------- ---------- ----------  ---------- ---------- ----------
eth1/0/1      0          0          0           0          0          0         0
eth1/0/2      0          0          0           0          0          0         0
eth1/0/3      0          0          0           0          0          0         0
eth1/0/4      0          0          0           0          0          0         0
eth1/0/5      0          0          0           0          0          0         0
eth1/0/6      0          0          0           0          0          0         0
eth1/0/7      0          0          0           0          0          0         0
eth1/0/8      0          0          0           0          0          0         0

Total Entries:8

Switch#
```

Отображаемые параметры

Rcv-Err	Обратитесь к «ifInErrors» в разделе «Отображаемые параметры» команды **show counters.**
UnderSize	Обратитесь к «rxUndersizedPkts» в разделе «Отображаемые параметры» команды **show counters.**
Xmit-Err	Обратитесь к «ifOutErrors» в разделе «Отображаемые

	параметры» команды **show counters.**
OutDiscard	Обратитесь к «ifOutDiscards» в разделе «Отображаемые параметры» команды **show counters**.
Single-Col	Обратитесь к «dot3StatsSingleColFrames» в разделе «Отображаемые параметры» команды **show counters**.
Multi-Col	Обратитесь к «dot3StatsMultiColFrames» в разделе «Отображаемые параметры» команды **show counters**.
Late-Col	Обратитесь к «dot3StatsLateCollisions» в разделе «Отображаемые параметры» команды **show counters**.
Excess-Col	Обратитесь к «dot3StatsExcessiveCollisions» в разделе «Отображаемыепараметры» команды **show counters.**
Symbol-Err	Обратитесь к «rxSymbolErrors» в разделе «Отображаемые параметры» команды **show counters**.
DeferredTx	Обратитесь к «txDelayExceededDiscards» в разделе «Отображаемые параметры» команды **show counters**.
IntMacTx	Обратитесь к «dot3StatsInternalMacTransmitErrors» в разделе «Отображаемые параметры» команды **show counters**.
IntMacRx	Обратитесь к пункту "dot3StatsInternalMacReceiveErrors" в команде **show counters**.
Align-Err	Обратитесь к пункту "dot3StatsAlignmentErrors" в команде **show counters**.
Fcs-Err	Обратитесь к пункту "dot3StatsFCSErrors" в команде **show counters**.

35-8 show interfaces status

Данная команда используется для просмотра состояния подключения портов коммутатора.

show interfaces [*INTERFACE-ID* **[, | -]] status**

Параметры

INTERFACE-ID	(Опционально) Укажите interface ID. Если параметр не указан, отображаться будет состояние подключения всех портов коммутатора.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду для отображения состояния подключения портов коммутатора. Если параметр не указан, будет отображено состояние подключения всех портов коммутатора.

Пример

В данном примере показано, как включить отображение состояния подключения портов коммутатора.

```
Switch# show interfaces eth1/0/1-8 status

Port          Status        VLAN         Duplex  Speed          Type
------------ ------------- ------------ ------- -------------- -------------
eth1/0/1      not-connected 1            auto    auto           1000BASE-T
eth1/0/2      not-connected 1            auto    auto           1000BASE-T
eth1/0/3      not-connected 1            auto    auto           1000BASE-T
eth1/0/4      not-connected 1            auto    auto           1000BASE-T
eth1/0/5      not-connected 1            auto    auto           1000BASE-T
eth1/0/6      not-connected 1            auto    auto           1000BASE-T
eth1/0/7      not-connected 1            auto    auto           1000BASE-T
eth1/0/8      connected     trunk        a-full  a-1000         1000BASE-T

Total Entries: 8

Switch#
```

35-9 show interfaces utilization

show interfaces [*INTERFACE-ID* **[, | -]] utilization**

Параметры

INTERFACE-ID	(Опционально) Укажите interface ID. Если параметр не указан, отображаться будет информация о загрузке всех физических портов коммутатора.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
utilization	(Опционально) Укажите для отображения информации о загрузке.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду для отображения загрузки портов коммутатора.

Пример

В данном примере показано отображение информации о загрузке портов коммутатора.

```
Switch# show interfaces utilization

Port        TX packets/sec  RX packets/sec   Utilization
----------- --------------  --------------   -----------
eth1/0/1      0               0                0
eth1/0/2      1488109         0                50
eth1/0/3      0               0                0
eth1/0/4      0               1488109          50
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#
```

35-10 show interfaces gbic

Данная команда используется для просмотра информации о состоянии GBIC.

show interfaces [*INTERFACE-ID* **[, | -]] gbic**

Параметры

INTERFACE-ID	(Опционально) Укажите interface ID. Если параметр не указан, отображаться будет информация о состоянии GBIC для всех интерфейсов GBIC.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
gbic	Отображение информации о состоянии GBIC.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для просмотра информации о состоянии GBIC.

Пример

В данном примере показано отображение информации о состоянии GBIC.

```
Switch#show interfaces ethernet 1/0/1 gbic

eth1/0/1
 Interface Type: 1000BASE-T


Switch#
```

35-11 show interfaces auto-negotiation

Данная команда используется для просмотра подробной информации об автосогласовании на физическом порту.

show interfaces [*INTERFACE-ID* **[, | -]] auto-negotiation**

Параметры

INTERFACE-ID	(Опционально) Укажите interface ID. Если параметр не указан, отображаться будет информация обо всех физических портах.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
auto-negotiation	Укажите для отображения подробной информации об автосогласовании.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для просмотра детальной информации об автосогласовании.

Пример

В данном примере показано отображение информации об автосогласовании.

```
Switch# show interfaces eth1/0/1-2 auto-negotiation

eth1/0/1
 Auto Negotiation: Disabled

eth1/0/2
 Auto Negotiation: Enabled

 Speed auto downgrade: Disabled
 Remote Signaling: Detected
 Configure Status: Configuring
 Capability Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
 Capability Advertised Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
 Capability Received Bits: -
 RemoteFaultAdvertised: Disabled
 RemoteFaultReceived: NoError

Switch#
```

35-12 show interfaces description

Данная команда используется для просмотра описания и состояния интерфейсов.

show interfaces [*INTERFACE-ID* **[, | -]] description**

Параметры

INTERFACE-ID	(Опционально) Укажите interface ID. Если параметр не указан, отображаться будет информация о всех интерфейсах.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.

-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
description	Укажите для отображения описания и состояния интерфейсов.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для просмотра описания и состояния интерфейсов.

Пример

В данном примере показано отображение описания и состояния 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         Pysical 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
```

35-13 shutdown

Данная команда используется для отключения интерфейса. При использовании формы **no** включит включит интерфейс.

shutdown
no shutdown

Параметры

Нет

По умолчанию

По умолчанию выбрана опция **no shutdown.**

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться для отключения интерфейсов физического порта, loopback, VLAN, Tunnel и интерфейсов управления. Команда также может использоваться для портов port- channel.

Команда отключает порт. В отключенном состоянии порт не будет принимать или 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 порт 1/0/1 с помощью данной команды.

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

36. Команды Internet Group Management Protocol (IGMP) Snooping

36-1 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

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#
```

36-2 ip igmp snooping

Данная команда используется для включения функции IGMP Snooping на коммутаторе. Используйте форму **no**, чтобы отключить данную функцию.

ip igmp snooping
no ip igmp snooping

Параметры

Нет

По умолчанию

Функция IGMP Snooping отключена на всех интерфейсах VLAN.
Функция IGMP Snooping отключена глобально.

Режим ввода команды

VLAN Configuration Mode
Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

В режиме Interface Configuration Mode команда может быть использована только для настройки интерфейса VLAN. Для того, чтобы предоставить VLAN доступ к IGMP Snooping, необходимо включить данную функцию глобально и для интерфейса. Настройки IGMP Snooping и MLD Snooping являются независимыми и могут быть применены для VLAN одновременно.

Пример

В данном примере показано, как отключить функцию IGMP Snooping на всех VLAN.

```
Switch# configure terminal
Switch(config)# no ip igmp snooping
Switch(config)#
```

В данном примере показано, как включить функцию IGMP Snooping на всех VLAN.

```
Switch# configure terminal
Switch(config)# ip igmp snooping
Switch(config)#
```

В данном примере показано, как отключить функцию IGMP Snooping на VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# no ip igmp snooping
Switch(config-vlan)#
```

36-3 ip igmp snooping fast-leave

Данная команда используется для настройки функции IGMP Snooping Fast Leave на интерфейсе. Используйте форму **no**, чтобы отключить данную функцию на указанном интерфейсе.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Используйте команду **ip igmp snooping fast-leave**, 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)#
```

36-4 ip igmp snooping last-member-query-interval

Данная команда используется для настройки интервала, через который IGMP snooping querier посылает IGMP сообщения с запросами, специфичными для группы или источника группы (канала). Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Получив сообщение IGMP Leave, IGMP Snooping Querier будет считать, что на интерфейсе нет локальных участников, если по истечении времени ожидания не будет получено ни одного ответа. Пользователи могут уменьшить данный интервал, чтобы сократить время, которое уходит у коммутатора на обнаружение потери последнего участника 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)#
```

36-5 ip igmp snooping mrouter

Эта команда используется для настройки указанного интерфейса(ов) в качестве портов маршрутизатора многоадресной рассылки или запрещенных портов маршрутизатора многоадресной рассылки на коммутаторе. Используйте форму **no** этой команды, чтобы удалить интерфейс(ы) из портов маршрутизатора или запрещенных портов маршрутизатора многоадресной рассылки.

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 не настроен.

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. 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. Если автоматическое изучение отключено, multicast router-порт может быть только сконфигурирован статически.

Пример

В этом примере показано, как добавить порт статического маршрутизатора многоадресной рассылки IGMP snooping для VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping mrouter interface eth4/0/1
Switch(config-vlan)#
```

36-6 ip igmp snooping proxy-reporting

Данная команда используется для включения функции Proxy Reporting. Используйте форму **no**, чтобы отключить данную функцию.

ip igmp snooping proxy-reporting [source *IP-ADDRESS***]**
no ip igmp snooping proxy-reporting

Параметры

source *IP-ADDRESS*	(Опционально) Укажите IP-адрес источника (source) Proxy Reporting. Значение по умолчанию составляет 0.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Когда функция прокси-отчета включена, полученные несколько пакетов IGMP report или leave для определенного (S, G) будут объединены в один отчет перед отправкой на порт маршрутизатора. IP-адрес источника proxy reporting source будет использоваться в качестве IP-адреса источника отчета, нулевой IP-адрес будет использоваться, если IP-адрес источника proxy reporting source не установлен.

Пример

В данном примере показано, как включить IGMP Snooping Proxy Reporting на VLAN 1 и настроить IP- адрес источника сообщения Proxy Reporting. Настроенный IP-адрес – 1.2.2.2.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-if)# ip igmp snooping proxy-reporting source 1.2.2.2
Switch(config-if)#
```

36-7 ip igmp snooping querier

Данная команда используется для указания устройства в качестве IGMP Snooping Querier. Используйте форму **no**, чтобы отключить данную функцию.

ip igmp snooping querier
no ip igmp snooping querier

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если система может играть роль querier, она будет прослушивать пакеты IGMP-запросов, отправленные другими устройствами. Если сообщение запроса IGMP получено, устройство с меньшим 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)#
```

36-8 ip igmp snooping query-interval

Данная команда используется для настройки интервала между сообщениями IGMP General Query. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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 31744.

По умолчанию

Значение по умолчанию – 125 секунд.

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. 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)#
```

36-9 ip igmp snooping query-max-response-time

Данная команда используется для настройки максимального значения времени ожидания, анонсированного в сообщениях IGMP Snooping Query. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Используйте данную команду, чтобы настроить период времени, в течение которого участник группы может ответить на сообщение IGMP Query, прежде чем его участие будет удалено посредством IGMP Snooping.

Пример

В данном примере показано, как настроить максимальное значение времени ожидания на интерфейсе. 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)#
```

36-10 ip igmp snooping query-version

Данная команда используется для настройки версии пакетов General Query, отправляемых IGMP Snooping Querier. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ip igmp snooping query-version *NUMBER*
no ip igmp snooping query-version

Параметры

NUMBER	Укажите версию пакета IGMP General Query, отправленного IGMP Snooping Querier. Доступный диапазон значений: от 1 до 3.

По умолчанию

Значение по умолчанию – 3.

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. 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)#
```

36-11 ip igmp snooping report-suppression

Данная команда используется для включения функции report suppression. Используйте форму **no**, чтобы отключить данную функцию.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. 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)#
```

36-12 ip igmp snooping robustness-variable

Данная команда используется для настройки robustness variable (переменной надежности), используемой в IGMP Snooping. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Robustness variable обеспечивает точную настройку в соответствии с ожидаемой потерей пакетов на интерфейсе. 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 Queries (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)#
```

36-13 ip igmp snooping static-group

Данная команда используется для настройки статической группы IGMP Snooping. Используйте форму **no**, чтобы удалить статическую группу.

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 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для создания статической группы IGMP snooping в случае, если подключенный хост не поддерживает протокол IGMP.

Пример

В данном примере показано, как добавить запись статической группы и источник multicast потока для IGMP Snooping.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping static-group 226.1.2.3 interface ethernet 1/0/5
Switch(config-vlan)#
```

36-14 ip igmp snooping suppression-time

Данная команда используется для настройки интервала, в течение которого будут блокированы дублированные сообщения IGMP Report или IGMP Leave. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ip igmp snooping suppression-time *SECONDS*
no ip igmp snooping suppression-time

Параметры

SECONDS	Укажите интервал блокирования дублированных сообщений IGMP Report. Доступный диапазон значений: от 1 до 300.

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Функция report suppression блокирует дублированные пакеты IGMP Report или IGMP Leave, полученные в течение указанного интервала. Чем меньше значение интервала suppression, тем чаще будут отправляться дублированные IGMP-пакеты.

Пример

В данном примере показано, как настроить интервал suppression на VLAN 1000. Указанное значение – 125.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping suppression-time 125
Switch(config-vlan)#
```

36-15 ip igmp snooping minimum-version

Данная команда используется для настройки минимальной версии IGMP-узлов, разрешенной на интерфейсе. Используйте форму **no**, чтобы удалить ограничение.

ip igmp snooping minimum-version {2 | 3}
no ip igmp snooping minimum-version

Параметры

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта настройка применяется только для фильтрации отчетов о членстве в IGMP.

Пример

В данном примере показано, как ограничить подключение всех узлов IGMPv1.

```
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.

```
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)#
```

36-16 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду для отображения информации IGMP snooping для всех VLAN, где IGMP snooping включен.

Пример

В данном примере показано, как отобразить настройки IGMP Snooping.

```
Switch#show ip igmp snooping

IGMP snooping global state: Enabled

Switch#
```

В этом примере показано, как отобразить информацию IGMP snooping для VLAN 2.

```
Switch#show ip igmp snooping vlan 2

    IGMP snooping state              : Disabled
    Minimum version                  : v1
    Fast leave                       : Enabled (host-based)
    Report suppression               : Disabled
    Suppression time                 : 10 seconds
    Querier state                    : Enabled (Non-active)
    Query version                    : v2
    Query interval                   : 300 seconds
    Max response time                : 20 seconds
    Robustness value                 : 2
    Last member query interval       : 3 seconds
    Proxy reporting                  : Enabled (Source 1.2.2.2)

Switch#
```

36-17 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***]**

Параметры

vlan *VLAN-ID*	(Опционально) Укажите интерфейс VLAN, который будет отображаться. Если VLAN не указан, будет отображаться информация о группах IGMP snooping всех VLAN.
IP-ADDRESS	(Опционально) Указывает IP-адрес группы, который будет отображаться. Если IP-адрес не указан, будет отображаться вся информация о группе IGMP.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду для отображения информации о группе IGMP snooping.

Пример

В этом примере показано, как отобразить информацию о группе IGMP snooping.

```
Switch# show ip igmp snooping groups

IGMP Snooping Connected Group Membership:

VLAN ID  Group address    Source address   FM  Exp(sec)  Interface
-------  ---------------  ---------------  --  --------  ---------
1        239.255.255.250        *          EX  382       2/0/7

Total Entries: 1

Switch#
```

Отображаемые параметры

FM	Filter Mode (Режим фильтрации): Значение режима фильтрации может быть либо IN (Включить), либо EX (Исключить). EX - Режим фильтрации - Исключить. IN - Режим фильтрации - Включить.
Exp (sec)	**Expire time** (Время истечения): Время в секундах до истечения срока действия записи.

36-18 show ip igmp snooping mrouter

Данная команда используется для отображения информации о многоадресном маршрутизаторе IGMP Snooping, который был автоматически изучен и настроен вручную.

show ip igmp snooping mrouter [vlan *VLAN-ID* **[, | -]]**

Параметры

vlan *VLAN-ID*	(Опционально) Указывает VLAN. Если VLAN не указана, будет отображаться информация IGMP snooping по всем 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

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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 IGMP Snooping.

```
Switch# show ip igmp snooping mrouter

VLAN     Ports
-------- ---------------------------------
1        3/0/3-3/0/4 (static)
         3/0/6 (forbidden)
         4/0/2 (dynamic)
2        4/0/4 (static)
         4/0/3 (dynamic)

Total Entries: 2

Switch#
```

36-19 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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
-------  ---------------  ------------------------
2        226.1.2.2        1/0/3

Total Entries: 1

Switch#
```

36-20 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 *INTERFACE-ID*	Указывает интерфейс для отображения счетчиков статистики порта.
vlan *VLAN-ID*	Указывает идентификатор VLAN для отображения статистики VLAN.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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#
```

37. Команды IP-MAC-Port Binding (IMPB)

37-1 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для удаления неразрешенных записей IMPB из базы данных фильтрации.

Пример

В данном примере показано, как удалить заблокированную запись на Ethernet 1/0/4.

```
Switch# clear ip ip-mac-port-binding violation interface ethernet 1/0/4
Switch#
```

37-2 ip ip-mac-port-binding

Данная команда используется для включения управления доступом IMPB для интерфейсов порта. При использовании формы **no** команда отключит функцию управления доступом IMPB.

ip ip-mac-port-binding [*MODE***]**
no ip ip-mac-port-binding

Параметры

MODE	Укажите режим управления доступом IMPB. **strict-mode:** укажите для включения строгого 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

Уровень команды по умолчанию

Уровень 12

Использование команды

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 Ethernet 1/0/10.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/10
Switch(config-if)# ip ip-mac-port-binding strict
Switch(config-if)#
```

37-3 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) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы

	до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
violation	(Опционально) Укажите для отображения заблокированной записи.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду для отображения настроек IMPB или 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#
```

37-4 snmp-server enable traps ip-mac-port-binding

Данная команда используется для включения уведомлений SNMP для привязки IP-MAC-Port Binding. При использовании формы **no** команда отключит уведомления SNMP.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

При включении данной функции коммутатор будет отправлять трапы при нарушениях безопасности, если будет получен некорректный пакет. Используйте эту команду для включения или отключения отправки уведомлений SNMP для таких событий.

Пример

В данном примере показано, как включить отправку трапов для IP-MAC-Port Binding.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps ip-mac-port-binding
Switch(config)#
```

38. Команды IP Multicast (IPMC)

38-1 show ip mroute forwarding-cache

Эта команда используется для отображения содержимого базы данных кэша перенаправления многоадресной маршрутизации IP.

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) Указывает IP-адрес источника многоадресной рассылки.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Кэш пересылки IP multicast представляет собой сводку таблицы маршрутов IP multicast, таблицы членов групп IGMP snooping и портов маршрутизаторов multicast.

Пример

В этом примере показано, как отобразить кэш переадресации многоадресной маршрутизации IP.

```
Switch#show ip mroute forwarding-cache
(10.1.1.1, 239.0.0.0) VLAN0060
  Outgoing interface list: 1/0/1, T2

(*,225.0.0.0) VLAN0070
  Outgoing interface list: 1/0/1-1/0/2

(10.1.1.1, 239.0.0.1) VLAN0060
  Outgoing interface list: 1/0/1, 2/0/2

Total entries: 3

Switch#
```

Отображаемые параметры	
239.0.0.0	Адрес группы.
10.1.1.1	Адрес источника.
*	Адрес источника с подстановочным знаком.
VLAN0060	Интерфейс, на который поступили многоадресные данные.
Outgoing interface list	Список исходящих интерфейсов для многоадресных данных. Он содержит интерфейсы коммутации 2-го уровня и маршрутизации 3-го уровня.

38-2 ip multicast table-lookup-mode

Эта команда используется для настройки режима поиска пересылки IP-мультикастинга. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

ip multicast table-lookup-mode {ip | mac}
no ip multicast table-lookup-mode

Параметры

ip	Указывает, что поиск переадресации многоадресной рассылки осуществляется на основе IP-адреса.
mac	Указывает, что поиск переадресации многоадресной рассылки осуществляется на основе MAC-адреса.

По умолчанию

По умолчанию эта функция основана на IP-адресе.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для настройки режима переадресации **IP multicasting forwarding lookup**.

Пример

В этом примере показано, как настроить режим переадресации IP multicasting forwarding lookup на mac.

```
Switch#configure terminal
Switch(config)#ip multicast table-lookup-mode mac
Switch(config)#
```

38-3 show ip multicast

Эта команда используется для отображения информации о многоадресной рассылке.

show ip multicast

Параметры

Нет

По умолчанию

Нет

Режим команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду для отображения информации об интерфейсе IP multicast.

Пример

В этом примере показано, как отобразить глобальное состояние маршрутизации многоадресной рассылки IP и режим поиска пересылки многоадресной рассылки IP.

```
Switch#show ip multicast

Table lookup mode: MAC

Switch#
```

39. Команды IP Multicast версии 6 (IPMCv6)

39-1 show ip mroute forwarding-cache

Эта команда используется для отображения содержимого базы данных кэша пересылки многоадресной маршрутизации IPv6.

show ipv6 mroute forwarding-cache [group-addr *GROUP-ADDRESS* **[source-addr** *SOURCE-ADDRESS***]]**

Параметры

group-addr *GROUP-ADDRESS*	(Опционально) Указывает IPv6-адрес группы.
source-addr *SOURCE-ADDRESS*	(Опционально) Указывает IPv6-адрес источника многоадресной рассылки.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Кэш пересылки многоадресной рассылки IPv6 представляет собой сводку таблицы маршрутов многоадресной рассылки IPv6, таблицы членов групп MLD snooping и портов маршрутизаторов многоадресной рассылки.

Пример

В этом примере показано, как отобразить кэш пересылки многоадресной маршрутизации IPv6.

```
Switch# show ipv6 mroute forwarding-cache

(2000:60:1:1::10, FF0E::1:1:1) VLAN0060
  Outgoing interface list: 1/0/1, port-channel2

(2000:60:1:1::10, FF0E::1:1:2) VLAN0060
  Outgoing interface list: 1/0/1, 2/0/2

Total entries: 2

Switch#
```

Отображаемые параметры

FF0E::1:1:1	Адрес группы.
2000:60:1:1::10	Адрес источника.
VLAN0060	Интерфейс, на который поступили многоадресные данные.
Outgoing interface list	Список исходящих интерфейсов для многоадресных данных. Он содержит интерфейсы коммутации 2-го уровня и маршрутизации 3-го уровня.

40. Команды IP Source Guard

40-1 ip verify source vlan dhcp-snooping

Данная команда используется для включения IP Source Guard на порту. При использовании формы **no** команда отключит IP Source Guard.

ip verify source vlan dhcp-snooping [ip-mac]
no ip verify source vlan dhcp-snooping [ip-mac]

Параметры

ip-mac	(Опционально) Укажите для проверки и IP, и MAC-адреса получаемых IP-пакетов.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для настройки 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 списка управления доступом (порт ACL) – аппаратный механизм. Его записи могут быть настроены вручную либо получены с помощью таблицы привязки DHCP. Пакет, не прошедший проверку, будет отброшен.

Существует два типа проверки:
- Если не указан ip-mac, проверка основана только на IP-адресе источника и VLAN.
- Если указан ip-mac, проверка основана на MAC-адресе источника, VLAN и IP-адресе источника.

Пример

В данном примере показано, как включить IP Source Guard для Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config-if)#
```

40-2 ip source binding

Данная команда используется для создания статической записи для IP Source Guard. При использовании формы **no** команда удалит статическую запись привязки.

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-ADDRESS	Укажите IP-адрес для привязки IP-to-MAC.
interface *INTERFACE-ID*	Укажите порт, к которому подключен проверенный узел.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для создания статической привязки, используемой для проверки IP Source Guard. При использовании формы no команда удалит статическую привязку. 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. Интерфейсом, указанным для команды, может быть физический порт или port-channel.

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 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 ethernet 1/0/10
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 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 ethernet
1/0/10
Switch(config)#
```

40-3 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) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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 настроить отображение привязки IP Source Guard без каких-либо параметров.

```
Switch#show ip source binding

MAC Address       IP Address      Lease(sec)  Type         VLAN Interface
----------------- --------------- ---------- ------------ ---- ---------
00-01-01-01-01-01 10.1.1.10        infinite  static       100  eth1/0/3
00-01-01-01-01-10 10.1.1.11          3120    dhcp-snooping 100  eth1/0/3

Total Entries: 2

Switch#
```

В данном примере показано, как настроить отображение привязки IP Source Guard для IP-адреса 10.1.1.10.

```
Switch# show ip source binding 10.1.1.10

MAC Address       IP Address      Lease(sec)  Type         VLAN   Interface
----------------- --------------- ---------- ------------ ----- ----------
00-01-01-01-01-01 10.1.1.10        infinite  static       100    eth1/0/3

Total Entries: 1

Switch#
```

В данном примере показано, как настроить отображение привязки IP Source Guard для IP-адреса 10.1.1.11, MAC-адреса 00-01-01-01-01-10 в VLAN 100 на Ethernet 1/0/3 и изучение DHCP Snooping.

```
Switch# show ip source binding 10.1.1.10 00-01-01-01-01-10 dhcp-snooping vlan 100 interface
eth1/0/3

MAC Address       IP Address      Lease(sec)  Type         VLAN   Interface
----------------- --------------- ---------- ------------ ----- -----------
00-01-01-01-01-10 10.1.1.11          3564    dhcp-snooping 100    eth1/0/3

Total Entries: 1

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.

40-4 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 настройки.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения записей списка управления доступом (ACL) аппаратного порта на определенном интерфейсе в таблице оборудования.

Пример

В данном примере показано, как настроить отображение, когда включен DHCP Snooping в VLAN 100 – 110, интерфейс в режиме IP Source Filter Mode настроен как IP, существующая привязка произведена к порту 10.1.1.1 в VLAN 100.

```
Switch#show ip verify source interface ethernet 1/0/3

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 настроить отображение, если интерфейс в режиме IP Source Filter Mode настроен как IP MAC, существующая привязка IP MAC привязывает IP-адрес 10.1.1.10 к MAC- адресу 00-01-01-01-01-01 в VLAN 100 и IP-адрес 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 активнойпроверки записей IP Source. **inactive-no-snooping-vlan:** не настроено DHCP Snooping в VLAN, нет активнойпроверки записей IP Source.
IP address	IP-адрес клиента, назначенный DHCP-сервером или настроенный пользователем
MAC address	MAC-адрес клиента.
VLAN	Номер VLAN интерфейса клиента.

41. Команды IP Utility

41-1 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.
IP-ADDRESS	Укажите IPv4-адрес узла назначения (destination).
ipv6	(Опционально) Укажите, чтобы использовать IPv6-адрес.
IPV6-ADDRESS	Укажите IPv6-адрес системы, который необходимо обнаружить.
HOST-NAME	Укажите имя узла системы, которое необходимо обнаружить.
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 адреса назначения и IP-адреса источника должен быть один тип — IPv4 или IPv6.

По умолчанию

Значение **count** отключено. Пинг будет продолжаться до тех пор, пока пользователь не завершит процесс. Значение **timeout** составляет 1 секунду.

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы проверить доступность, надежность и задержку маршрута к узлу назначения. Если не выбран параметр **count** или **timeout**, остановить Ping можно только используя комбинацию клавиш Ctrl+C.

Пример

В этом примере показано, как пинговать узел с IP-адресом 211.21.180.1 со счетом 4 раза.

```
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 протестировать 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#
```

41-2 ping access-class

Данная команда используется для указания списка доступа, который ограничит доступ для Ping. Используйте форму **no**, чтобы удалить проверку при помощи списка доступа.

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

Параметры

IP-ACL	Укажите стандартный список доступа IP. Поле адреса источника (source) разрешающей или запрещающей записи определяет, действителен узел, или нет.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда задает список доступа для ограничения доступа через ping. Для выполнения команды указанный список доступа не обязательно должен существовать.

Пример

В этом примере показано, как создать ping access-class, который используется для ограничения ping только с узла 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)#
```

41-3 traceroute

Данная команда используется для отображения пути передачи от узла к узлу через сеть IP от коммутатора к указанному узлу назначения (destination).

traceroute {[ip] *IP-ADDRESS* **| [ipv6]** *IPV6-ADDRESS* **|** *HOST-NAME***} [length** *LENGTH***] [probe** *NUMBER***] [timeout** *SECONDS***] [max-ttl** *TTL***] [port** *DEST-PORT***]**

Параметры

ip	(Опционально) Укажите, чтобы использовать IPv4-адрес.
IP-ADDRESS	Укажите IPv4-адрес узла назначения.
ipv6	(Опционально) Укажите, чтобы использовать IPv6-адрес.
IPV6-ADDRESS	Укажите IPv6-адрес системы, который необходимо обнаружить.
HOST-NAME	Укажите имя узла системы, которое необходимо обнаружить.
Probe *NUMBER*	(Опционально) Укажите количество дейтаграмм, которое необходимо отослать. Доступный диапазон значений: от 1 до 9.
timeout *SECONDS*	(Опционально) Укажите время ожидания ответа в секундах.
max-ttl *TTL*	(Опционально) Укажите максимальное значение TTL для исходящих UDP-дейтаграмм. Максимальный доступный диапазон значений: от 1 до 60.
port *DEST-PORT*	(Опционально) Укажите количество базовых UDP-портов назначения, используемых в исходящих дейтаграммах.

	Значение увеличивается при отправке каждой дейтаграммы. Допустимый диапазон для порта назначения: от 1 до 65535. Используйте данную опцию в маловероятных событиях, если узел назначения прослушивает порт в диапазоне портов Trace Route по умолчанию.

По умолчанию

По умолчанию эта команда отправляет дейтаграммы со значением TTL, равным 1.
По умолчанию максимальное значение TTL равно 30, период тайм-аута - 5 секунд, номер порта UDP - 33434, а номер запроса для каждого TTL - 1.

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Чтобы прервать выполнение данной команды, используйте сочетание клавиш Ctrl+C.

Данная команда использует поле TTL в IP-заголовке, чтобы маршрутизаторы и серверы могли генерировать определенные ответные сообщения (Return messages). **Traceroute** запускается при отправке UDP-дейтаграммы на узел назначения с полем TTL 1. Если маршрутизатор обнаруживает значение TTL 1 или 0, дейтаграмма будет отброшена, а отправителю будет выслано ответное сообщение об истечении времени ответа (ICMP Time Exceeded). **Traceroute** определяет адрес первого узла при проверке поля адреса источника (source) сообщения ICMP Time Exceeded.

Чтобы идентифицировать следующий узел, **traceroute** снова отправляет UDP-пакет, но в этот раз значение TTL равно 2. Первый маршрутизатор уменьшает поле TTL на 1 и отправляет дейтаграмму на следующий маршрутизатор. Обнаружив TTL со значением 1, второй маршрутизатор отбрасывает дейтаграмму и отправляет на источник сообщение Time Exceeded. Этот процесс продолжается до тех пор, пока значение TTL не увеличится настолько, чтобы дейтаграмма могла достичь узла назначения (или до тех пор, пока не будет достигнуто максимальное значение TTL).

Чтобы определить, достигла ли дейтаграмма своего назначения, **traceroute** устанавливает очень большое значение для UDP-порта назначения в дейтаграмме, так что оно вряд ли будет использоваться узлом назначения. Если узел получает дейтаграмму с нераспознанным номером порта, на источник будет отправлена ошибка ICMP Port Unreachable. Данное сообщение свидетельствует **traceroute** о том, что дейтаграмма достигла назначения.

Пример

В данном примере показана трассировка узла с IP-адресом 211.21.180.1.

```
Switch#traceroute 211.21.180.1

 10  ms  10.1.1.254
 30  ms  192.168.249.134
 30  ms  192.168.249.134
 <10 ms  192.168.5.230
 <10 ms  211.21.180.1

Trace complete.


Switch#
```

В данном примере В этом примере показана трассировка хоста с IPv6-адресом 2001:238:f8a:77:7c10:41c0:6ddd:ecab., как выполнить трассировку маршрута к узлу 172.50.71.123, при этом маршрутизатор не отвечает.

```
Switch#traceroute 2001:238:f8a:77:7c10:41c0:6ddd:ecab

 10  ms  1001:238:f8a:77:7c10:41c0:6ddd:ecab

Trace complete.


Switch#
```

41-4 ip helper-address

Данная команда используется для того, чтобы добавить адрес назначения для передачи пакетов UDP Broadcast. Используйте форму **no**, чтобы удалить адрес назначения передачи.

ip helper-address *IP-ADDRESS*
no ip helper-address [*IP-ADDRESS***]]**

Параметры

IP-ADDRESS	Укажите IP-адрес назначения для передачи пакетов UDP Broadcast.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для конфигурирования интерфейса VLAN. Используйте данную команду, чтобы контролировать передачу пакетов UDP Broadcast. Команда действует только в том случае, если полученному интерфейсу присвоен IP-адрес.

Система передает только те пакеты, которые соответствуют следующим требованиям:

- MAC-адрес назначения (destination) должен быть широковещательным адресом.
- IP-адрес назначения должен быть широковещательным адресом.
- Тип пакетов – IPv4 UDP.
- Значение IP TTL должно быть больше или равно 2.

Пример

В данном примере показано, как сконфигурировать адрес IP Helper для VLAN 100. Указанный адрес – 172.50.71.123.

```
Switch# configure terminal
Switch(config)#interface vlan 100
Switch(config-if)#ip helper-address  172.50.71.123
Switch(config-if)#
```

41-5 ip forward-protocol

Данная команда используется для включения передачи пакетов UDP определенного типа службы. Используйте форму **no**, чтобы отключить передачу пакетов UDP определенного типа службы.

ip forward-protocol udp [*PORT***]**
no ip forward-protocol udp [*PORT***]**

Параметры

PORT	Указывает порт назначения службы UDP, который должен быть перенаправлен или нет.

По умолчанию

По умолчанию включены часто используемые протоколы приложений.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Ниже представлен список часто используемых протоколов приложений, которые будут переданы по умолчанию, если адрес IP Helper сконфигурирован. Если команда или форма no данной команды сконфигурирована без указания номера порта, будут применены порты по умолчанию. Порт 67 и порт 68 BOOTP UDP указать нельзя, так как пакеты передаются при помощи DHCP Relay. Ниже перечислены порты по умолчанию:

- Порт 69 Trivial File Transfer Protocol (TFTP).
- Порт 53 Domain Naming System (DNS).
- Порт 37 Time service.
- Порт 137 NetBIOS Name Server.
- Порт 138 NetBIOS Datagram Server.
- Порт 49 TACACS service.
- Порт 42 IEN-116 Name Service.

Пример

В этом примере показано, как отключить перенаправление IP-помощника на порт UDP 53 (DNS).

```
Switch#configure terminal
Switch(config)#no ip forward-protocol udp 53
Switch(config)#
```

41-6 show ip helper-address

Данная команда используется для отображения таблицы адресов UDP Helper.

show ip helper-address [*INTERFACE-ID***]**

Параметры

INTERFACE-ID	(Опционально) Указывает отображение для указанного интерфейса VLAN.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду для отображения всех целевых адресов для пересылки широковещательных пакетов UDP, или укажите идентификатор VLAN для отображения целевых адресов для интерфейса VLAN.

Пример

В этом примере показано, как отобразить все адреса помощников.

```
Switch#show ip helper-address

Interface   Helper-address
----------  ---------------
vlan100     172.50.71.123

Switch#
```

41-7 show ip forward-protocol udp

Данная команда используется для отображения информации обо всех указанных UDP-портах.

show ip forward-protocol udp

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию обо всех указанных UDP-портах.

Пример

В данном примере показано, как отобразить информацию обо всех указанных UDP-портах.

```
Switch#show ip forward-protocol udp

Application                 UDP Port
--------------------        ---------------
Time Service                37
IEN-116 Name Service        42
TACACS                      49
TFTP                        69
NetBIOS-NS                  137
NetBIOS-DS                  138

Switch#
```

42. Команды IPv6 Snooping

42-1 ipv6 snooping policy

Данная команда используется для создания или изменения политики IPv6 Snooping Policy. Команда позволяет войти в режим IPv6 Snooping Configuration Mode. При использовании формы **no** данная команда удаляет IPv6 Snooping Policy.

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 Policy не создано.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для создания политики IPv6 Snooping Policy и входа в режим IPv6 Snooping Configuration Mode. 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)#
```

42-2 protocol

Данная команда используется для указания протокола, для которого необходимо применить IPv6 Snooping. 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 все протоколы отключены.

Режим ввода команды

IPv6 Snooping Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Функция Neighbor Discovery (ND) Snooping создана для автонастройки адресов IPv6 без аутентификации и адресов IPv6, настроенных вручную. Перед назначением адреса IPv6, узел должен сначала выполнить Duplicate Address Detection (DAD). ND Snooping обнаруживает сообщения DAD, включающие DAD Neighbor Solicitation (NS) и DAD Neighbor Advertisement (NA), для построения таблицы привязки. NDP-пакет (NS и NA) также используется для определения того, доступен ли узел по-прежнему и можно ли удалить привязку или нет.

DHCPv6 Snooping анализирует DHCPv6-пакеты, отправляемые между DHCPv6-клиентом и сервером во время процедуры назначения адреса. Когда DHCPv6-клиент успешно получает корректный IPv6- адрес, DHCPv6 Snooping создает его таблицу привязки.

DHCP-PD Snooping анализирует пакеты DHCPv6 Prefix Delegation (PD) между Delegating Router (назначенным IPv6-префиксом) и соответствующим Requesting Router для настройки привязки префикса.

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)#
```

42-3 limit address-count

Данная команда используется для ограничения максимального количества привязок IPv6 Snooping. При использовании формы **no** данная команда вернется в значения по умолчанию.

limit address-count *MAXIMUM*
no limit address-count

Параметры

MAXIMUM	Укажите максимальное количество привязок IPv6 Snooping. Доступен диапазон значений от 0 до 511.

По умолчанию

По умолчанию ограничений нет.

Режим ввода команды

IPv6 Snooping Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для ограничения количества привязок IPv6 Snooping, для которых применяется политика IPv6 Sooping Policy. Команда помогает ограничить размер таблицы привязки.

Пример

В данном примере показано, как задать максимальное число 25 для привязки IPv6 Snooping.

```
Switch# configure terminal
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# limit address-count 25
Switch(config-ipv6-snooping)#
```

42-4 ipv6 snooping attach-policy

Данная команда используется для применения политики IPv6 Snooping Policy к указанной VLAN. При использовании формы **no** данная команда удалит привязку.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

После создания политики IPv6 Snooping Policy используйте данную команду для применения политики к определенной VLAN.

Пример

В данном примере показано, как создать включить IPv6 Snooping в VLAN 200.

```
Switch#configure terminal
Switch(config)#vlan 200
Switch(config-vlan)#ipv6 snooping attach-policy policy1
Switch(config-vlan)#
```

42-5 ipv6 snooping station-move deny

Данная команда используется для запрета функции Station Move для привязки IPv6 Snooping. При использовании формы **no** данная команда вернется к значениям по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

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)#
```

42-6 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для просмотра информации о DHCPv6 Guard. Если параметр не указан, отображаться будет информация для всех политик.

Пример

В данном примере показано, как включить отображение информации о DHCPv6 Guard.

```
Switch# show ipv6 snooping policy

Snooping policy: test1
        Protocol: DHCP, NDP
        Limit Address Count: 30
        Target VLAN: 100,200-210,4000

Switch#
```

Отображаемые параметры

Protocol	Протокол, используемый для Snooping.
Limit Address Count	Максимально допустимое число записей для данной политики IPv6 Snooping Policy.
Target VLAN	Имя списка VLAN.

43. Команды IPv6 Source Guard

43-1 ipv6 source binding vlan

Данная команда используется для добавления статической записи в таблицу привязки. При использовании формы **no** данная команда удалит статическую привязку.

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-ID	Укажите VLAN привязки, созданной вручную.
IPV6-ADDRESS	Укажите IPv6-адрес привязки, созданной вручную.
INTERFACE-ID	Укажите номер интерфейса привязки, созданной вручную.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для добавления статической записи в таблицу привязки вручную. Для данной команды указанная VLAN необязательно должна существовать. Если указанный интерфейс позже будет удален, настройки команды будут соответственно также удалены.

Пример

В данном примере показано, как настроить привязку IPv6 Source Guard с адресом IPv6 2000::1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 на Ethernet 1/0/10.

```
Switch# configure terminal
Switch(config)# ipv6 source binding 00-01-02-03-04-05 vlan 2 2000::1 interface ethernet 1/0/1
Switch(config)#
```

43-2 ipv6 source-guard policy

Данная команда используется для создания политики IPv6 Source Guard Policy. Команда позволяет войти в режим IPv6 Source-Guard Policy Configuration Mode. При использовании формы **no** данная команда удалит политику IPv6 Source Guard Policy.

ipv6 source-guard policy *POLICY-NAME*

no ipv6 source-guard policy *POLICY-NAME*

Параметры

POLICY-NAME	Укажите имя политики IPv6 Source Guard Policy.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для создания политики IPv6 Source Guard Policy. Команда позволяет войти в режим IPv6 Source-Guard Policy Configuration Mode.

Пример

В данном примере показано, как создать политику IPv6 Source Guard Policy.

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy policy1
Switch(config-source-guard)#
```

43-3 deny global-autoconfig

Данная команда используется для запрета автоматически сконфигурированного трафика. При использовании формы **no** команда отключит данную функцию.

deny global-autoconfig
no deny global-autoconfig

Параметры

Нет

По умолчанию

По умолчанию данная опция разрешена.

Режим ввода команды

Source-Guard Policy Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для запрета трафика от автоматически сконфигурированных глобальных адресов. Она может использоваться, когда 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)#
```

43-4 permit link-local

Данная команда используется для аппаратного разрешения трафика данных, отправленного с адреса Link-Local. При использовании формы **no** команда отключит данную функцию.

permit link-local
no permit link-local

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Source-Guard Policy Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для аппаратного разрешения трафика данных, отправленного с дреса Link-Local.

Пример

В данном примере показано, как разрешить весь трафик данных, отправленный 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)#
```

43-5 ipv6 source-guard attach-policy

Данная команда используется для применения IPv6 Source Guard на интерфейсе. При использовании формы **no** данная команда удалит IPv6 Source Guard с интерфейса.

ipv6 source-guard attach-policy [*POLICY-NAME***]**
no ipv6 source-guard attach-policy

Параметры

POLICY-NAME	(Опционально) Укажите имя политики Source Guard Policy.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Когда команда применена к порту, принятый IPv6-пакет, кроме ND, RA, RS и DHCP-сообщений будет выполнять проверку привязки адреса. Пакет будет разрешен, если он соответствует любой записи в таблице привязки адресов. Таблица привязки 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, по умолчанию политика Source Guard Policy разрешит пакеты, отправленные с помощью автоматически сконфигурированного адреса, и запретит пакеты, отправленные с адреса Link-Local.

Пример

В этом примере показано применение политики защиты источника IPv6 "pol1" к порту 3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ipv6 source-guard attach-policy pol1
Switch(config-if)#
```

43-6 show ipv6 source-guard policy

Данная команда используется для просмотра настроек IPv6 Source Guard Policy.

show ipv6 source-guard policy [*POLICY-NAME***]**

Параметры

POLICY-NAME	(Опционально) Укажите имя политики Source Guard Policy.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для просмотра настроек IPv6 Source Guard Policy. Если имя политики не указано, отображаться будет информация для всех политик IPv6 Source Guard.

Пример

В этом примере показано, как отобразить конфигурацию политики защиты источников IPv6.

```
Switch# show ipv6 dhcp guard policy

Policy Test configuration:
    permit link-local
    deny global-autoconf
    Target: eth1/0/3

Switch#
```

43-7 show ipv6 neighbor binding

Данная команда используется для просмотра таблицы привязки 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 адресу IPv6.
mac *MAC-ADDRESS*	(Опционально) Укажите для отображения привязок, соответствующих указанному MAC-адресу.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Команда используется для просмотра таблицы привязки.

Пример

В данном примере показано, как включить отображение указанных записей из таблицы привязки.

```
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.

44. Команды японского веб-контроля доступа (JWAC)

44-1 jwac authentication-method

Эта команда используется для настройки метода аутентификации JWAC. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

jwac authentication-method {chap | md5 | mschap | mschapv2 | pap}
no jwac authentication-method

Параметры

chap	Указывает, что аутентификация будет осуществляться через сервер RADIUS через CHAP.
md5	Указывает, что аутентификация будет осуществляться через сервер RADIUS посредством EAP MD5.
mschap	Указывает, что аутентификация будет осуществляться через сервер RADIUS посредством MS-CHAP.
mschapv2	Указывает, что аутентификация будет осуществляться через сервер RADIUS посредством MS-CHAPv2.
pap	Указывает, что аутентификация будет осуществляться через сервер RADIUS по протоколу PAP.

По умолчанию

По умолчанию методом аутентификации JWAC является PAP.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для указания протокола RADIUS, который JWAC использует для завершения аутентификации RADIUS.

Пример

В этом примере показано, как настроить метод аутентификации JWAC на MS-CHAPv2.

```
Switch# configure terminal
Switch(config)# jwac authentication-method mschapv2
Switch(config)#
```

44-2 jwac enable

Эта команда используется для включения функции JWAC на порту. Используйте форму **no** этой команды, чтобы отключить JWAC на порту.

jwac enable
no jwac enable

Параметры

Нет

По умолчанию

По умолчанию эта опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда конфигурации интерфейса JWAC позволяет узлам, подключенным к порту, выполнять аутентификацию через веб-браузер.

Пример

В этом примере показано, как включить функцию JWAC на интерфейсе eth1/0/1.

```
Switch# configure terminal
Switch(config)# jwac virtual-ip ipv4 1.1.1.1
Switch(config)# jwac virtual-ip url www.website1.com
Switch(config)# jwac success redirect-path http://www.website2.com
Switch(config)# jwac redirect destination jwac-login-page
Switch(config)# jwac system-auth-control
Switch(config)# interface eth1/0/1
Switch(config-if)# jwac enable
Switch(config-if)#
```

44-3 jwac forcible-logout

Эта команда используется для включения функции принудительного выхода из системы JWAC. Используйте форму **no** этой команды для отключения функции принудительного выхода из системы JWAC.

jwac forcible-logout
no jwac forcible-logout

Параметры

Нет

По умолчанию

По умолчанию эта опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Когда функция принудительного выхода из системы включена, пакет ping от аутентифицированного хоста к коммутатору JWAC с TTL 1 и IP-адресом назначения, совпадающим с виртуальным IP-адресом, будет рассматриваться как запрос на выход из системы, и хост будет переведен обратно в состояние без аутентификации.

Пример

В этом примере показано, как включить функцию принудительного выхода из системы JWAC.

```
Switch# configure terminal
Switch(config)# jwac forcible-logout
Switch(config)#
```

44-4 jwac max-authenticating-user

Эта команда используется для настройки максимального числа аутентифицирующих пользователей на указанном интерфейсе. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

jwac max-authenticating-user *NUMBER*
no jwac max-authenticating-user

Параметры

NUMBER	Указывает для установки максимального количества аутентифицируемых пользователей. Диапазон составляет от 1 до 100.

По умолчанию

По умолчанию это значение равно 100.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для настройки максимального числа аутентифицирующих пользователей для JWAC на указанном интерфейсе.

Пример

В этом примере показано, как настроить максимальное число аутентифицирующих пользователей для JWAC на 10 на интерфейсе eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# jwac max-authenticating-user 10
Switch(config-if)#
```

44-5 jwac authenticate-page language

Эта команда используется для выбора языка страницы аутентификации. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

jwac authenticate-page language {japanese | english}
no jwac authenticate-page language

Параметры

japanese	Указывает на выбор японской страницы.
english	Указывает на выбор страницы на английском языке.

По умолчанию

По умолчанию этот параметр - английский.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Веб-сервер JWAC вернет страницу аутентификации клиенту для локальной аутентификации. Существуют японская и английская версии для этих страниц аутентификации. По умолчанию используется английская версия. Используйте эту команду, чтобы выбрать язык страницы аутентификации JWAC.

Пример

В этом примере показано, как изменить язык страницы аутентификации JWAC на японский.

```
Switch# configure terminal
Switch(config)# jwac authenticate-page language japanese
Switch(config)#
```

44-6 jwac page-element

Эта команда используется для настройки элементов страницы аутентификации JWAC. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

jwac page-element {japanese | english} {page-title *STRING* **| login-window-title** *STRING* **| username-title** *STRING* **| password-title** *STRING* **| logout-window-title** *STRING* **| copyright- line** *LINE-NUMBER* **title** *STRING***}**
no jwac page-element {japanese | english} {page-title | login-window-title | username-title | password-title | logout-window-title | copyright-line}

Параметры

japanese	Указывает на настройку элемента японской страницы.
english	Указывает на настройку элемента страницы на английском языке.
page-title *STRING*	Указывает заголовок страницы аутентификации JWAC. Максимальное количество может составлять до 128 символов.
login-window-title *STRING*	Указывает заголовок окна входа в систему аутентификации JWAC. Максимальное число может составлять до 64 символов.
username-title *STRING*	Указывает заголовок имени пользователя в окне входа в систему аутентификации JWAC. Максимальное количество может составлять до 32 символов.
password-title *STRING*	Указывает заголовок пароля окна входа в систему аутентификации JWAC. Максимальное количество может составлять до 32 символов.
logout-window-title *STRING*	Указывает заголовок окна выхода из аутентификации JWAC. Максимальное количество может составлять до 64 символов.
copyright- line *LINE-NUMBER* **title** *STRING*	Указывает информацию об авторских правах по строкам на страницах аутентификации JWAC. Всего информация об авторских правах может содержать до 5 строк и 128 символов для каждой строки.

По умолчанию

Это значения по умолчанию:
page-title - не задан.
login-window-title - "Вход в систему аутентификации".
username-title - "Имя пользователя".
password-title - "Пароль".
logout-window-title - "Выход из сети".
Информация об авторских правах не установлена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для настройки элементов страницы аутентификации JWAC. Существует две страницы аутентификации JWAC, (1) страница входа в аутентификацию и (2) страница выхода из аутентификации.

Страница входа в систему веб-аутентификации будет отображаться пользователю для получения имени пользователя и пароля, когда система выполняет веб-аутентификацию для пользователя. Пользователи могут выйти из сети, нажав кнопку **Logout** на странице входа в систему аутентификации после успешного входа в сеть.

Пример

В этом примере показано, как настроить заголовок страницы на " Company":

```
Switch# configure terminal
Switch(config)# jwac page-element english page-title Company
Switch(config)#
```

В этом примере показано, как настроить двухстрочную информацию об авторских правах в нижней части страницы аутентификации:
Line 1: Copyright @ 2020 Все права защищены
Line 2: Сайт: http://support.website.com

```
Switch# configure terminal
Switch(config)# jwac page-element english copyright-line 1 title Copyright @ 2020
All Rights Reserved
Switch(config)# jwac page-element english copyright-line 2 title Site:
http://support.website.com
Switch(config)#
```

44-7 jwac quarantine-server url

Эта команда используется для настройки URL-адреса карантинного сервера JWAC. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

jwac quarantine-server url {ipv4 *STRING* **| ipv6** *STRING***}**
no jwac quarantine-server url

Параметры

ipv4 *STRING*	Указывает URL-адрес карантинного сервера для аутентификации доступа IPv4. Максимальное число может составлять до 128 символов.
ipv6 *STRING*	Указывает URL-адрес сервера карантина для аутентификации доступа IPv6. Максимальное число может составлять до 128 символов.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда позволяет настроить URL-адрес карантинного сервера. Если перенаправление включено и местом назначения перенаправления является сервер карантина, при получении HTTP-запроса от неаутентифицированного узла, который не направляется на сервер карантина, коммутатор обработает этот HTTP-пакет и отправит обратно сообщение узлу, чтобы заставить его получить доступ к серверу карантина с настроенным URL. Когда ПК подключится к указанному URL, сервер карантина запросит пользователя ПК ввести имя пользователя и пароль для аутентификации.

Пример

В этом примере показано, как настроить URL-адрес карантинного сервера JWAC на "http://10.90.90.88/authpage.html".

```
Switch# configure terminal
Switch(config)# jwac quarantine-server url ipv4 http://10.90.90.88/authpage.html
Switch(config)#
```

В этом примере показано, как настроить URL-адрес карантинного сервера JWAC на "http://[3000::2]/authpage.html".

```
Switch# configure terminal
Switch(config)# jwac quarantine-server url ipv6 http://[3000::2]/authpage.html
Switch(config)#
```

44-8 jwac quarantine-server monitor

Эта команда используется для включения функции мониторинга сервера JWAC Quarantine. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

jwac quarantine-server monitor
no jwac quarantine-server monitor

Параметры

Нет

По умолчанию

По умолчанию эта опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Когда функция мониторинга карантинного сервера JWAC включена, коммутатор JWAC будет контролировать карантинный сервер, чтобы убедиться, что сервер в порядке. Если коммутатор обнаружит отсутствие сервера карантина, он перенаправит все неаутентифицированные HTTP доступы на страницу входа в JWAC, если опция перенаправления включена и назначение перенаправления настроено на сервер карантина.

Пример

В этом примере показано, как включить функцию сервера JWAC Quarantine.

```
Switch# configure terminal
Switch(config)# jwac quarantine-server monitor
Switch(config)#
```

44-9 jwac quarantine-server timeout

Эта команда используется для установки периода тайм-аута сервера JWAC Quarantine. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

jwac quarantine-server timeout *SECONDS*
no jwac quarantine-server timeout *SECONDS*

Параметры

SECONDS	Указывает период тайм-аута. Диапазон составляет от 5 до 300 секунд.

По умолчанию

По умолчанию это значение равно 30 секундам.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если включен монитор сервера карантина, коммутатор JWAC будет периодически проверять, работает ли сервер карантина. Если коммутатор не получает никакого ответа от сервера карантина в течение настроенного тайм-аута ошибки, коммутатор будет считать, что он работает некорректно.

Пример

В этом примере показано, как настроить период ожидания ошибки сервера JWAC Quarantine на 60 секунд.

```
Switch# configure terminal
Switch(config)# jwac quarantine-server timeout 60
Switch(config)#
```

44-10 jwac redirect

Эта команда используется для включения функции перенаправления JWAC или настройки назначения перенаправления и времени задержки. Используйте форму **no** этой команды, чтобы отключить перенаправление JWAC или вернуть параметры к настройкам по умолчанию.

jwac redirect [destination {quarantine-server | jwac-login-page} | delay-time *SECONDS*]
no jwac redirect [destination | delay-time]

Параметры

destination	(Опционально) Указывает место назначения, на которое будет перенаправлен неаутентифицированный узел.
delay-time *SECONDS*	(Опционально) Указывает период времени, по истечении которого неаутентифицированный хост будет перенаправлен. Единица измерения - секунды. Диапазон составляет от 0 до 10 секунд.

По умолчанию

По умолчанию JWAC перенаправляет на страницу входа в систему JWAC.
По умолчанию время задержки составляет 1 секунду.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если указано перенаправление на сервер карантина, неаутентифицированный узел будет перенаправлен на сервер карантина при попытке доступа к случайному URL. Если указано перенаправление на страницу входа JWAC, неаутентифицированный хост будет перенаправлен на страницу входа JWAC в коммутаторе для завершения аутентификации. Когда перенаправление включено, весь веб-доступ перенаправляется на карантинный сервер или страницу входа JWAC. Если указано перенаправление на сервер карантина, то перед глобальным включением функции JWAC необходимо сначала настроить сервер карантина. Когда перенаправление отключено, весь веб-доступ запрещен, кроме доступа к серверу карантина или странице входа JWAC.

Пример

В этом примере показано, как включить функцию перенаправления JWAC.

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

В этом примере показано, как настроить назначение перенаправления JWAC на сервер карантина.

```
Switch# configure terminal
Switch(config)# jwac redirect destination quarantine-serve
Switch(config)#
```

В этом примере показано, как настроить время задержки перенаправления JWAC на 5 секунд.

```
Switch# configure terminal
Switch(config)# jwac redirect delay-time 5
Switch(config)#
```

44-11 jwac system-auth-control

Эта команда используется для глобального включения функции JWAC на коммутаторе. Используйте форму **no** этой команды чтобы отключить функцию JWAC глобально на коммутаторе.

jwac system-auth-control
no jwac system-auth-control

Параметры

Нет

По умолчанию

По умолчанию эта опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

JWAC - это функция, предназначенная для аутентификации пользователя, когда он пытается получить доступ к Интернету через коммутатор. Пользователь-клиент инициирует процесс аутентификации JWAC с помощью веб-доступа.

Пример

В этом примере показано, как включить функцию JWAC глобально на коммутаторе.

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

44-12 jwac update-server

Эта команда используется для настройки сети сервера обновлений, к которой ПК должен получить доступ для завершения аутентификации JWAC. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

jwac update-server {*IPV4-PREFIX/PREFIX–LENGTH* **|** *IPV6-PREFIX/PREFIX-LENGTH***} [tcp** *NUMBER* **| udp** *NUMBER***]**

no jwac update-server {*IPV4-PREFIX/PREFIX–LENGTH* **|** *IPV6-PREFIX/PREFIX-LENGTH***} [tcp** *NUMBER* **| udp** *NUMBER***]**

Параметры

IPV4-PREFIX/PREFIX–LENGTH	Указывает сетевой адрес IPv4 для сети сервера обновлений.
IPV6-PREFIX/PREFIX-LENGTH	Указывает сетевой адрес IPv6 для сети сервера обновлений.
tcp *NUMBER*	(Опционально) Укажите номер доступного TCP-порта для указанной сети сервера обновлений.
udp *NUMBER*	(Опционально) Укажите номер доступного порта UDP для указанной сети сервера обновлений.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для добавления или удаления сетевого адреса сервера, на который трафик от неаутентифицированного клиентского узла не будет блокироваться коммутатором JWAC. Любые серверы (например, update.microsoft.com или некоторые сайты компаний-производителей антивирусного программного обеспечения, к которым ActiveX должен получить доступ для выполнения аутентификации перед прохождением аутентификации клиентом) должны быть добавлены со своим IP-адресом или с сетевым адресом. Добавление сетевого адреса позволяет обслуживать несколько серверов обновлений в одной сети. Можно настроить несколько адресов серверов обновлений или сетевых адресов.

Пример

В этом примере показано, как добавить сервер обновления JWAC с сетевым адресом 10.90.90.0/24 и портом TCP 80.

```
Switch# configure terminal
Switch(config)# jwac update-server 10.90.90.90/24 tcp 80
Switch(config)#
```

44-13 jwac udp-filtering

Эта команда используется для включения функции фильтрации JWAC UDP. Используйте форму **no** этой команды для отключения функции фильтрации JWAC UDP.

jwac udp-filtering
no jwac udp-filtering

Параметры

Нет

По умолчанию

По умолчанию эта опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Когда функция фильтрации UDP включена, все пакеты UDP и ICMP, за исключением пакетов DHCP и DNS от неаутентифицированных хостов, будут отбрасываться.

Пример

В этом примере показано, как включить функцию фильтрации JWAC UDP.

```
Switch# configure terminal
Switch(config)# jwac udp-filtering
Switch(config)#
```

44-14 jwac virtual-ip

Эта команда используется для настройки виртуального IP-адреса JWAC, который используется для обмена сообщениями с хостами. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

jwac virtual-ip {ipv4 *IP-ADDRESS* **| ipv6** *IPV6-ADDRESS* **| url** *STRING***}**
no jwac virtual-ip {ipv4 | ipv6 | url}

Параметры

ipv4 *IP-ADDRESS*	Указывает виртуальный IPv4-адрес JWAC.
ipv6 *IPV6-ADDRESS*	Указывает виртуальный IPv6-адрес JWAC.
url *STRING*	Указывает FQDN URL для JWAC FQDN URL. Он может содержать до 128 символов.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Виртуальный IP-адрес JWAC - это всего лишь характеристика функции JWAC на коммутаторе. Все процессы аутентификации JWAC взаимодействуют с этим IP-адресом, однако виртуальный IP не отвечает ни на ICMP-пакеты, ни на ARP-запросы. Поэтому нельзя настраивать виртуальный IP в той же подсети, что и IP-интерфейс коммутатора, или в той же подсети, что и подсеть хост-компьютеров, иначе аутентификация JWAC не сможет работать правильно.

Определенный URL вступает в силу только после настройки виртуального IP-адреса. Пользователи получают URL FQDN, хранящийся на DNS-сервере, чтобы получить виртуальный IP-адрес. Полученный IP-адрес должен совпадать с виртуальным IP-адресом, настроенным командой.

Если виртуальный IP-адрес IPv4 не настроен, доступ IPv4 не может запустить аутентификацию JWAC. Если виртуальный IPv6 не настроен, доступ IPv6 не может начать аутентификацию JWAC.

Пример

В этом примере показано, как настроить виртуальный IPv4 JWAC на "1.1.1.1" и FQDN URL на "www.web.co".

```
Switch# configure terminal
Switch(config)# jwac virtual-ip ipv4 1.1.1.1
Switch(config)# jwac virtual-ip url www.web.co
Switch(config)#
```

В этом примере показано, как настроить виртуальный IPv6 JWAC на "2000::2" и FQDN URL на "www.web.co".

```
Switch# configure terminal
Switch(config)# jwac virtual-ip ipv6 2000::2
Switch(config)# jwac virtual-ip url www.web.co
Switch(config)#
```

45. Команды Jumbo Frame

45-1 max-rcv-frame-size

Данная команда используется для настройки максимально допустимого размера Ethernet-фреймов. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

max-rcv-frame-size *BYTES*
no max-rcv-frame-size

Параметры

BYTES	Укажите максимально допустимый размер Ethernet-фреймов. Доступный диапазон значений: от 64 до 12288 байт.

По умолчанию

Значение по умолчанию – 1536 байт.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для конфигурирования физических портов. Фреймы избыточного размера будут отброшены, на входных портах будут проведены проверки. Используйте данную команду, чтобы передавать большие фреймы или jumbo-фреймы через коммутатор и оптимизировать передачу от сервера к серверу.

Пример

В данном примере показано, как настроить максимальный размер полученных Ethernet-фреймов на порту 1/0/3. Указанное значение – 6000 байт.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/3
Switch(config-if)#max-rcv-frame-size 6000
Switch(config-if)#
```

46. Команды Link Aggregation Control Protocol (LACP)

46-1 channel-group

Данная команда используется для привязки интерфейса к аггрегированной группе (channel-group). Используйте форму **no**, чтобы удалить интерфейс из аггрегированной группы (channel-group).

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется 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.

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 ethernet 1/0/4-1/0/5
Switch(config-if)# channel-group 3 mode active
Switch(config-if)#
```

46-2 lacp port-priority

Данная команда используется для настройки приоритета порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

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 ethernet 1/0/4-1/0/5
Switch(config-if)# lacp port-priority 20000
Switch(config-if)#
```

46-3 lacp timeout

Данная команда используется для настройки таймера LACP Long или LACP Short. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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, и 1 секунду для интервала между регулярными передачами LACP PDU. Данный параметр применяется, если канал-партнер использует Short Timeouts.
long	Укажите, чтобы выбрать значение 90 секунд для интервала, по истечении которого полученная информация о LACPDU будет объявлена недействительной, и 30 секунд для интервала между регулярными передачами LACP PDU. Данный параметр применяется, если канал-партнер использует Long Timeouts.

По умолчанию

Режим LACP Timeout по умолчанию – Short.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 ethernet 1/0/1
Switch(config-if)# lacp timeout long
Switch(config-if)#
```

46-4 lacp system-priority

Данная команда используется для настройки приоритета системы. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Во время LACP-согласования локальный партнер обменивается с удаленным партнером приоритетом системы и приоритетом порта. 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)#
```

46-5 port-channel load-balance

Данная команда используется для настройки алгоритма Load Balancing (балансировка нагрузки), используемого коммутатором для распределения пакетов на порты одного канала. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

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)#
```

46-6 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Если номер port-channel не указан, будут отображены все port-channel. Если в команде **show channel- group** не указаны параметры **channel**, **load-balance** и **sys-id**, 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
  ------------------------------------------------
  eth3/0/8      N/A    bndl         N/A        N/A
  eth3/0/9      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#
```

47. Команды Link Layer Discovery Protocol (LLDP)

47-1 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. Доступны только физические интерфейсы.
,	(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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

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#
```

47-2 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-ID	Укажите interface ID. Доступны только физические интерфейсы.
,	(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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если в команде не указан параметр **interface**, будет удалена вся информация, полученная от соседних устройств, на всех интерфейсах.

Пример

В данном примере показано, как удалить всю информацию, полученную от соседних устройств, на всех интерфейсах.

```
Switch# clear lldp table all
Switch#
```

47-3 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. Используйте форму **no**, чтобы отключить передачу TLV.

lldp dot1-tlv-select {port-vlan | protocol-vlan *VLAN-ID* **[, | -] | vlan-name [***VLAN-ID* **[, | -]] | proto-col-identity [***PROTOCOL-NAME***]}**

no lldp dot1-tlv-select {port-vlan | protocol-vlan [*VLAN-ID* **[, | -]] | 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.
protocol-vlan	Укажите PPVID (Port and Protocol VLAN ID) TLV, который необходимо отправить. PPVID TLV – это дополнительный TLV, который позволяет порту Bridge анонсировать PPVID.
VLAN-ID	Укажите VLAN ID в PPVID TLV. Доступный диапазон значений: от 1 до 4094. Если VLAN ID не указан, все сконфигурированные PPVID VLAN будут удалены, PPVID 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.
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.
proto-col-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 **gvrp** - GARP VLAN Registration Protocol **stp** - Spanning Tree Protocol

По умолчанию

По умолчанию указанные в пределах IEEE 802.1 TLV не заданы.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для конфигурирования физических портов. 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.

PPVID TLV будет отправлен на VLAN только при условии, что сконфигурированный VLAN ID соответствует настройкам Protocol VLAN на данном интерфейсе, а данная VLAN существует. 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 ethernet 1/0/1
Switch(config-if)# lldp dot1-tlv-select port-vlan
Switch(config-if)#
```

В данном примере показано, как включить анонсирование Port and Protocol VLAN ID TLV. Анонсированные VLAN: от VLAN 1 до VLAN 3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp dot1-tlv-select protocol-vlan 1-3
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 ethernet 1/0/1
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 ethernet 1/0/1
Switch(config-if)# lldp dot1-tlv-select protocol-identify lacp
Switch(config-if)#
```

47-4 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. Используйте форму **no**, чтобы отключить передачу TLV.

lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | power | max-frame-size]
no lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | power | 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.
power	(Необязательно) Указывает TLV питания через MDI для отправки. Три реализации IEEE 802.3 PMD (10BASE-T, 100BASE-TX и 1000BASE-T) позволяют подавать питание по каналу для подключенных систем без питания. Power Via MDI TLV позволяет сетевому управлению рекламировать и обнаруживать возможности поддержки питания MDI отправляющей станции локальной сети IEEE 802.3.
max-frame-size	(Опционально) Укажите Maximum Frame Size TLV, который необходимо отправить. Maximum Frame Size TLV указывает максимальный размер фрейма для используемого MAC и PHY.

По умолчанию

По умолчанию указанный в пределах IEEE 802.3 TLV не указан.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для конфигурирования физических портов. 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.

Если не указаны дополнительные параметры, будут выбраны все поддерживаемые TLV, указанные в пределах IEEE 802.3, или выбор всех TLV, указанных в пределах IEEE 802, будет отменен.

Пример

В данном примере показано, как включить анонсирование MAC/PHY Configuration/Status TLV.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp dot3-tlv-select mac-phy-cfg
Switch(config-if)#
```

47-5 lldp fast-count

Данная команда используется для настройки количества отправляемых пакетов Fast Start (LLDP MED Fast Start Repeat Count Option) на коммутаторе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

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 этом примере показано, как настроить счетчик повторов быстрого запуска LLDP MED.

```
Switch# configure terminal
Switch(config)# lldp fast-count 10
Switch(config)#
```

47-6 lldp hold-multiplier

Данная команда используется для того, чтобы настроить множитель удержания для обновлений LLDP на коммутаторе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

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)#
```

47-7 lldp management-address

Данная команда используется для настройки адреса управления (Management Address), который будет анонсирован на физическом интерфейсе. Используйте форму **no**, чтобы удалить заданные настройки.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для конфигурирования физических портов. 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 этом примере показано, как настроить IPv4-адрес управления на портах 1 - 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 этом примере показано, как настроить IPv6-адрес управления на портах 4-6.

```
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 этом примере показано, как удалить управляющий IPv4-адрес с портов 1 - 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 этом примере показано, как удалить управляющий IPv6-адрес с портов 4-6.

```
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 этом примере показано, как удалить все управляющие IPv4/IPv6-адреса с порта 5. С порта 5 не будет отправляться TLV адресов управления.

```
Switch# configure terminal
Switch(config)# interface eth1/0/5
Switch(config-if)# no lldp management-address
Switch(config-if)#
```

47-8 lldp med-tlv-select

Данная команда используется для указания дополнительного LLDP-MED TLV, который будет передан, инкапсулипрован в LLDPDU и отправлен на соседние устройства. Используйте форму **no**, чтобы отключить передачу TLV.

lldp med-tlv-select [capabilities | inventory-management | network-policy | power-management]
no lldp med-tlv-select [capabilities | inventory-management | network-policy | power-management]

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.
power- management	(Опционально) Указывает передавать LLDP-MED расширенную мощность через MDI TLV, если локальное устройство является PSE-устройством или PD-устройством.

По умолчанию

LLDP-MED TLV по умолчанию не выбран.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для конфигурирования физических портов. 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 ethernet 1/0/1
Switch(config-if)# lldp med-tlv-select capabilities
Switch(config-if)#
```

47-9 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для конфигурирования 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 ethernet 1/0/1
Switch(config-if)# lldp receive
Switch(config-if)#
```

47-10 lldp reinit

Данная команда используется для настройки минимального интервала перед повторной инициализацией на коммутаторе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

47-11 lldp run

Данная команда используется для глобального включения функции LLDP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

lldp run
no lldp run

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

47-12 lldp forward

Данная команда используется для включения состояния LLDP Forwarding. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

lldp forward
no lldp forward

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

47-13 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. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для конфигурирования 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 ethernet 1/0/1
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 ethernet 1/0/1
Switch(config-if)# lldp tlv-select system-name
Switch(config-if)#
```

47-14 lldp transmit

Данная команда используется для включения анонсирования/передачи LLDP. Используйте форму **no**, чтобы отключить передачу LLDP.

lldp transmit
no lldp transmit

Параметры

Нет

По умолчанию

По умолчанию передача LLDP включена на всех поддерживаемых интерфейсах.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для конфигурирования физических портов. 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 ethernet 1/0/1
Switch(config-if)# lldp transmit
Switch(config-if)#
```

47-15 lldp tx-delay

Данная команда используется для настройки таймера Transmission Delay, определяющего минимальный интервал между отправкой LLDP-сообщений на основе постоянно изменяющегося содержания MIB. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

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)#
```

47-16 lldp tx-interval

Данная команда используется для настройки интервала LLDPDU Transmission. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

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)#
```

47-17 snmp-server enable traps lldp

Данная команда используется для включения отправки LLDP Trap и LLDP-MED Trap. Используйте форму **no**, чтобы отключить данную функцию.

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

Уровень команды по умолчанию

Уровень 12

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)#
```

47-18 lldp notification enable

Данная команда используется для включения отправки уведомлений LLDP и LLDP-MED на интерфейсе. Используйте форму **no**, чтобы отключить данную функцию.

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

Уровень команды по умолчанию

Уровень 12

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 ethernet 1/0/1
Switch(config-if)# lldp med notification enable
Switch(config-if)#
```

47-19 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

Уровень команды по умолчанию

Уровень 12

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 ethernet 1/0/1
Switch(config-if)# lldp subtype port-id mac-address
Switch(config-if)#
```

47-20 show lldp

Данная команда используется для отображения общих настроек функции LLDP на коммутаторе.

show lldp

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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-68-36-30-B0
    System Name               : Switch
    System Description        : Gigabit Ethernet 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         : 1.00.001
    Software Revision         : 1.00.001
    Serial Number             : DGS3130111013
    Manufacturer Name         : D-Link Corporation
    Model Name                : DGS-3130-30TS Gigabit Ethernet S
    Asset ID                  :

LLDP Configurations
    LLDP State                : Disabled
    LLDP Forward State        : Disabled
    Message TX Interval       : 30
    Message TX Hold Multiplier: 4
    ReInit Delay              : 2
    TX Delay                  : 2

LLDP-MED Configuration:
    Fast Start Repeat Count   : 4


Switch#
```

47-21 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 interface ID, который необходимо отобразить. Доступны только физические интерфейсы.
,	(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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию о функции LLDP для каждого физического интерфейса.

Пример

В данном примере показано, как отобразить настройки функции LLDP для указанного физического интерфейса.

```
Switch#show lldp interface ethernet 1/0/1

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
    Link Aggregation                                    :Disabled
    Maximum Frame Size                                  :Disabled
    Energy Efficient Ethernet                           :Disabled

LLDP-MED Organizationally Specific TLVs:

    LLDP-MED Capabilities TLV                           :Disabled
    LLDP-MED Network Policy TLV                         :Disabled
    LLDP-MED Inventory TLV                              :Disabled

LLDP-DCBX Organizationally Specific TLVs:

    LLDP-DCBX ETS Configuration TLV                     :Disabled
    LLDP-DCBX ETS Recommendation TLV                    :Disabled
    LLDP-DCBX Priority-based Flow Control Configuration 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)».

47-22 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 interface ID. Доступны только физические интерфейсы.
,	(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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

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 ethernet 1/0/1 detail

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : eth1/0/1
Port Description                         : D-Link Corporation DGS-1510-28XMP
                                           HW A1 firmware 1.70.005 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                              : 1.3.6.1.4.1.171.10.137.9.1

    Address 2 :
        Subtype                          : IPv4
        Address                          : 10.90.90.90
        IF Type                          : IfIndex
        OID                              : 1.3.6.1.4.1.171.10.137.9.1

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 ethernet 1/0/1

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : eth1/0/1
Port Description                         : D-Link Corporation DGS-1510-28XMP
                                           HW A1 firmware 1.70.005 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)
Power Via MDI                            : (See Detail)
Link Aggregation                         : (See Detail)
Maximum Frame Size                       : 1536
LLDP-MED capabilities                    : (See Detail)
Network Policy                           : (See Detail)
Extended power via MDI                   : (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 ethernet 1/0/1 brief

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : eth1/0/1
Port Description                         : D-Link Corporation DGS-1510-28XMP
                                           HW A1 firmware 1.70.005 Port 1 on
                                           Unit 1


Switch#
```

47-23 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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                              : 1.3.6.1.4.1.171.10.137.9.1
    Advertising Ports                : -

Address 2 :
-----------------------------------------------
    Subtype                          : IPv4
    Address                          : 10.90.90.90
    IF Type                          : IfIndex
    OID                              : 1.3.6.1.4.1.171.10.137.9.1
    Advertising Ports                : -

Total Entries : 2

Switch#
```

47-24 show lldp neighbor 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 interface ID. Доступны только физические интерфейсы.
,	(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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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 eth1/0/9, 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 данном примере показано, как отобразить информацию о Remote LLDP в стандартном формате.

```
Switch#show lldp neighbors interface ethernet 1/0/9

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 этом примере показано, как отобразить информацию о соседе на eth1/0/9 в кратком режиме.

```
Switch#show lldp neighbors interface ethernet 1/0/9 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#
```

47-25 show lldp traffic

Данная команда используется для отображения глобальной информации о трафике LLDP.

show lldp traffic

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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.

47-26 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 interface ID. Доступны только физические интерфейсы.
,	(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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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 ethernet 1/0/1

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.

48. Команды Loopback Detection (LBD)

48-1 loopback-detection (Global)

Данная команда используется для того, чтобы включить функцию LBD (Loopback Detection) глобально. Используйте форму **no**, чтобы глобально отключить данную функцию.

loopback-detection [mode {port-based | vlan-based}]
no loopback-detection [mode]

Параметры

mode	(Опционально) Укажите режим обнаружения.
port-based	Укажите режим обнаружения петли port-based (на порту).
vlan-based	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

Уровень команды по умолчанию

Уровень 12

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-detec**t, 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)#
```

48-2 loopback-detection (Interface)

Данная команда используется для включения функции LBD на интерфейсе. Используйте форму **no**, чтобы отключить данную функцию на интерфейсе.

loopback-detection
no loopback-detection

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда доступна только для конфигурации физического порта и интерфейса порт-канала. Используйте эту команду для включения или отключения функции обнаружения обратной петли на интерфейсе.

Пример

В данном примере показано, как включить функцию LBD на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# loopback-detection
Switch(config-if)#
```

48-3 loopback-detection action

Данная команда используется для настройки режима LBD. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить режим LBD.

Пример

В этом примере показано, как настроить действие обнаружения шлейфа на **none**.

```
Switch# configure terminal
Switch(config)# loopback-detection action none
Switch(config)#
```

48-4 loopback-detection address-type

Данная команда используется для того, чтобы настроить тип адреса назначения (destination) пакетов LBD. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

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)#
```

48-5 loopback-detection interval

Данная команда используется для конфигурирования временного интервала. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

По умолчанию это значение равно 10 секундам

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

48-6 loopback-detection vlan

Данная команда используется для того, чтобы включить функцию LBD на VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

loopback-detection vlan *VLAN-LIST*
no loopback-detection vlan *VLAN-LIST*

Параметры

VLAN-LIST	Укажите идентификационный номер / номера / диапазон номеров VLAN. Чтобы указать список диапазонов VLAN, введите одно или несколько значений, разделяя их при помощи запятых или дефисов.

По умолчанию

По умолчанию данная опция включена для всех VLAN.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команд

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)#
```

48-7 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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.
State	Отображает статус порта.
Result	Отображает, обнаружена ли петля.
Time Left	Отображает время, оставшееся до автовосстановления.

48-8 snmp-server enable traps loopback-detection

Данная команда используется для включения отправки SNMP-уведомлений для LBD. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить отправку SNMP-уведомлений для LBD. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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)#
```

49. Команды аутентификации MAC

49-1 mac-auth system-auth-control

Данная команда используется для глобального включения MAC-аутентификации. При использовании формы **no** команда отключит глобальную MAC-аутентификацию.

mac-auth system-auth-control
no mac-auth system-auth-control

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

MAC-аутентификация – это функция, предназначенная для аутентификации пользователя на основе MAC-адреса при попытке доступа к сети через коммутатор. Сам коммутатор может выполнять аутентификацию на основе локальной базы данных или выполнять процесс аутентификации для клиентов на удаленном сервере с использованием протокола RADIUS.

Пример

В данном примере показано, как включить MAC-аутентификацию глобально.

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

49-2 mac-auth enable

Данная команда используется для включения MAC-аутентификации на указанном интерфейсе. При использовании формы **no** команда отключит MAC-аутентификацию.

mac-auth enable
no mac-auth enable

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда доступна только для настройки интерфейса физического порта. Она может использоваться для включения MAC-аутентификации на указанном интерфейсе.

Также MAC-аутентификация имеет следующие ограничения:

- MAC-аутентификация на порту не может быть включена, если на данном порту включена функция Port Security.
- MAC-аутентификация на порту не может быть включена, если на данном порту включена функция IP-MAC-Port-Binding.
- MAC-аутентификация на порту не может быть включена на порту, где настроено агрегирование каналов.

Пример

В данном примере показано, как включить MAC-аутентификацию на Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# mac-auth enable
Switch(config-if)#
```

49-3 mac-auth password

Данная команда используется для настройки пароля аутентификации для локальной и RADIUS-аутентификации. При использовании формы **no** команда вернется к значениям по умолчанию.

mac-auth password [0 | 7] *STRING*
no mac-auth password

Параметры

0	(Опционально) Пароль в обычном текстовом виде. Если не указан ни 0, ни 7, по умолчанию пароль будет в обычном текстовом виде.
7	(Опционально) Зашифрованный пароль. Если не указан ни 0, ни 7, по умолчанию пароль будет в обычном текстовом виде.
password *STRING*	Укажите, чтобы задать пароль для MAC-аутентификации. Если указан пароль в обычном текстовом виде, длина

	строки не может превышать 16 символов.

По умолчанию

По умолчанию паролем является MAC-адрес клиента.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для настройки пароля, используемого для аутентификации пользователей по MAC-адресу. Если команда не настроена, пароль для аутентификации пользователя по MAC-адресу будет сформирован на основе MAC-адреса. Формат MAC-адреса может быть настроен с помощью команды **authentication mac username format**.

Пример

В данном примере показано, как настроить пароль MAC-аутентификации.

```
Switch# configure terminal
Switch(config)# mac-auth password newpass
Switch(config)#
```

49-4 mac-auth username

Данная команда используется для настройки имени пользователя для локальной и RADIUS- аутентификации. При использовании формы **no** команда вернется к значениям по умолчанию.

mac-auth username *STRING*
no mac-auth username

Параметры

STRING	Укажите, чтобы задать имя пользователя для MAC-аутентификации. Длина строки не может превышать 16 символов.

По умолчанию

По умолчанию именем пользователя является MAC-адрес клиента.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для настройки имени пользователя для аутентификации пользователей по MAC-адресу. Это имя пользователя используется для аутентификации через локальную базу данных и удаленные серверы. Если команда не настроена, имя пользователя для аутентификации будет формироваться на основе MAC-адреса.

Пример

В данном примере показано, как настроить имя пользователя для MAC-аутентификации.

```
Switch# configure terminal
Switch(config)# mac-auth username dlink
Switch(config)#
```

49-5 snmp-server enable traps mac-auth

Данная команда используется для включения отправки SNMP-уведомлений для MAC-аутентификации. При использовании формы **no** команда отключит SNMP-уведомления.

snmp-server enable traps mac-auth
no snmp-server enable traps mac-auth

Параметры

Нет

По умолчанию

По умолчанию функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду, чтобы включить или отключить отправку SNMP-уведомлений для MAC-аутентификации.

Пример

В данном примере показано, как включить отправку трапов для MAC-аутентификации.

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

50. Команды Mirror

50-1 monitor session destination interface

Данная команда используется для того, чтобы настроить интерфейс назначения (destination) для сессии мониторинга, позволяя отслеживать пакеты на портах источника (source) через порт назначения. Используйте форму **no**, чтобы удалить интерфейс назначения сессии.

monitor session *SESSION-NUMBER* **destination interface** *INTERFACE-ID*
no monitor session *SESSION-NUMBER* **destination interface** *INTERFACE-ID*
no monitor session *SESSION-NUMBER*

Параметры

SESSION-NUMBER	Укажите номер сессии мониторинга. Доступный диапазон значений: от 1 до 4.
INTERFACE-ID	Укажите интерфейс назначения для сессии мониторинга.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для настройки интерфейса назначения для сеанса локального монитора.

В качестве интерфейсов назначения для сеансов мониторинга могут использоваться как физические порты, так и каналы портов. Для сеанса мониторинга можно указать несколько интерфейсов источника, но только один интерфейс назначения. Интерфейс не может быть одновременно интерфейсом источника одного сеанса и портом назначения другого сеанса. Интерфейс может быть настроен как интерфейс назначения нескольких сеансов, но может быть интерфейсом источника только одного сеанса.

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 ethernet 1/0/1
Switch(config)# monitor session 1 source interface ethernet 1/0/2-4
Switch(config)#
```

50-2 monitor session source interface

Данная команда используется для того, чтобы сконфигурировать порт источника (source) сессии мониторинга. Используйте форму **no**, чтобы удалить порт источника из сессии мониторинга.

monitor session *SESSION-NUMBER* **source interface** *INTERFACE-ID* **[, | -] [both | rx | tx [forwarding]]**
no monitor session *SESSION-NUMBER* **source interface** *INTERFACE-ID* **[, | -]**
no monitor session *SESSION-NUMBER*

Параметры

SESSION-NUMBER	Укажите номер сессии мониторинга. Доступный диапазон значений: 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.
forwarding	(Необязательно) Указывает отслеживать пакеты, передаваемые на порту, только когда статус всех STGs порта - forwarding.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 ethernet 1/0/1
Switch(config)# monitor session 1 source interface ethernet 1/0/2-4
Switch(config)#
```

50-3 monitor session source acl

Данная команда используется для того, чтобы сконфигурировать список доступа для мониторинга на основе потока. Используйте форму **no**, чтобы удалить список доступа для мониторинга на основе потока.

monitor session *SESSION-NUMBER* **source acl** *ACCESS-LIST-NAME*
no monitor session *SESSION-NUMBER* **source acl** *ACCESS-LIST-NAME*

Параметры

SESSION-NUMBER	Укажите номер сессии мониторинга. Доступный диапазон значений: от 1 до 4.
ACCESS-LIST-NAME	Укажите зеркалирование на основе потока.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команд

Одновременно можно отслеживать несколько списков доступа на сеансе.

Пример

В данном примере показано, как создать сессию мониторинга с номером 2. Список доступа MAC «MAC-Monitored-flow» указан в качестве источника мониторинга.

```
Switch# configure terminal
Switch(config)# monitor session 2 destination interface ethernet 1/0/1
Switch(config)# monitor session 2 source acl MAC-Monitored-flow
Switch(config)#
```

50-4 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.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду без указания номера сессии, чтобы отобразить все сессии мониторинга.

Пример

В данном примере показано, как отобразить сессию мониторинга порта с номером 1.

```
Switch# show monitor session 1

Session 1
   Session Type: local session
   Destination Port: Ethernet1/0/1
   Source Ports:
      Both:
          Ethernet1/0/2  (only for TX forwarding)
          Ethernet1/0/3  (only for TX forwarding)
          Ethernet1/0/4
      RX:
          Ethernet1/0/5
      TX:
          Ethernet1/0/7

Total Entries: 1

Switch#
```

51. Команды Multicast Listener Discovery (MLD) Snooping

51-1 clear ipv6 mld snooping statistics

Данная команда используется для сброса счетчиков статистики MLD Snooping на коммутаторе.

clear ipv6 mld snooping statistics {all | vlan *VLAN-ID* **| interface** *INTERFACE-ID***}**

Параметры

all	Укажите, чтобы очистить статистику IPv6 MLD Snooping для всех VLAN и портов.
vlan *VLAN-ID*	Укажите VLAN. Если VLAN не указана, будет очищена статистика всех VLAN.
interface *INTERFACE-ID*	Укажите интерфейс.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы сбросить счетчики статистики MLD Snooping на коммутаторе.

Пример

В данном примере показано, как очистить всю статистику MLD Snooping.

```
Switch# clear ipv6 mld snooping statistics all
Switch#
```

51-2 ipv6 mld snooping

Данная команда используется для включения MLD Snooping. Используйте форму no, чтобы отключить MLD Snooping.

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

VLAN Configuration Mode
Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Чтобы применить MLD Snooping на VLAN, необходимо включить глобальное состояние MLD Snooping и MLD Snooping на интерфейсе. Настройки IGMP Snooping и MLD Snooping являются независимыми, поэтому их можно включать одновременно на одной и той же VLAN.

Пример

В данном примере показано, как отключить MLD Snooping на всех VLAN.

```
Switch# configure terminal
Switch(config)# no ipv6 mld snooping
Switch(config)#
```

В данном примере показано, как включить MLD Snooping на VLAN, доступных для данной функции.

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping
Switch(config)#
```

В данном 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)#
```

51-3 ipv6 mld snooping fast-leave

Данная команда используется для включения функции MLD Snooping Fast Leave на интерфейсе. Используйте форму **no**, чтобы отключить функцию MLD Snooping Fast Leave на интерфейсе.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Используйте команду **ipv6 mld snooping fast-leave**, 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)#
```

51-4 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. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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. Доступныйдиапазон значений: от 1 до 25.

По умолчанию

Значение по умолчанию – 1 секунда.

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. 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. 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)#
```

51-5 ipv6 mld snooping mrouter

Данная команда используется для того, чтобы настроить указанный интерфейс в качестве порта IPv6, подключенного к многоадресному маршрутизатору, или порта, которому запрещено подключаться к многоадресному маршрутизатору, на интерфейсе VLAN. Используйте форму **no**, чтобы удалить интерфейс из списка портов, подключенных к маршрутизатору, или портов, которым запрещено подключаться к многоадресному маршрутизатору.

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 или список интерфейсов. Пробелы до и после запятой недопустимы. Доступны физические интерфейсы или port-channel.
,	(Опционально) Указывает серию интерфейсов или отделяет диапазон интерфейсов от предыдущего диапазона. До или после запятой пробел не допускается.
-	(Опционально) Указывает диапазон интерфейсов. До или после дефиса пробел не допускается.
learn pimv6	Укажите, чтобы включить динамическое изучение на портах, подключенных к многоадресному маршрутизатору.

По умолчанию

Порт IPv6, подключенный к многоадресному маршрутизатору, не настроен.
Автоматическое изучение включено.

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Чтобы указать порт маршрутизатора многоадресной рассылки, допустимым интерфейсом может быть физический порт или порт-канал. Указанный порт маршрутизатора многоадресной рассылки должен быть портом-членом сконфигурированной сети VLAN.

Порт многоадресного маршрутизатора может быть либо динамически обучаемым, либо статически настроенным на объект MLD snooping. При динамическом обучении устройство MLD snooping будет прослушивать пакеты MLD и PIMv6, чтобы определить, является ли партнерское устройство маршрутизатором.

Пример

В данном примере показано, как сконфигурировать интерфейс Ethernet 1/0/1 в качестве порта, подключенного к многоадресному маршрутизатору MLD Snooping, а интерфейс Ethernet 1/0/2 в качестве порта, не подключенного к многоадресному маршрутизатору MLD Snooping, на VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping mrouter interface ethernet 1/0/1
Switch(config-vlan)# ipv6 mld snooping mrouter forbidden interface ethernet 1/0/2
Switch(config-vlan)#
```

В данном примере показано, как отключить автоматическое изучение пакетов протокола маршрутизации.

```
Switch# configure terminal
Switch(config)# vlan 4
Switch(config-vlan)# no ipv6 mld snooping mrouter learn pimv6
Switch(config-vlan)#
```

51-6 ipv6 mld snooping proxy-reporting

Данная команда используется для включения функции Proxy Reporting. Используйте форму **no**, чтобы отключить данную функцию.

ipv6 mld snooping proxy-reporting [source *IPV6-ADDRESS***]**
no ipv6 mld snooping proxy-reporting

Параметры

source *IPV6-ADDRESS*	(Опционально) Укажите IP-адрес источника (source) Proxy

Reporting.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Функция Proxy Reporting работает только для трафика MLDv1.

Если функция Proxy Reporting включена, несколько полученных пакетов MLD Report или MLD Leave будут объединены в одно сообщение, а затем отправлены на порт, подключенный к маршрутизатору. IP-адрес источника Proxy Reporting будет использован в качестве IP-адреса источника сообщения.
Если IP-адрес источника Proxy Reporting не указан, будет использован нулевой IP-адрес. MAC-адрес интерфейса будет использован в качестве MAC-адреса источника сообщения. Если для VLAN не указан IP-адрес, будет использован системный MAC-адрес.

Пример

В данном примере показано, как включить MLD Snooping Proxy Reporting на VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping proxy-reporting
Switch(config-vlan)#
```

51-7 ipv6 mld snooping querier

Данная команда используется для включения MLD Snooping Querier на коммутаторе. Используйте форму **no**, чтобы отключить MLD Snooping Querier.

ipv6 mld snooping querier
no ipv6 mld snooping querier

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

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. Если на интерфейсе также включен MLD-протокол, состояние MLD Snooping Querier будет отключено автоматически.

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)#
```

51-8 ipv6 mld snooping query-interval

Данная команда используется для того, чтобы задать интервал отправки сообщений MLD General Query. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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. Доступный диапазон значений: от 1 до 31744.

По умолчанию

Значение по умолчанию – 125 секунд.

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Интервал MLD General Query – 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)#
```

51-9 ipv6 mld snooping query-max-response-time

Данная команда используется для настройки максимального времени ответа, анонсированного в запросах MLD Snooping Query. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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. Доступный диапазон значений: от 1 до 25 секунд.

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Команда применяется для настройки периода времени, в течение которого участник группы может ответить на сообщение MLD Query. После истечения данного периода его участие в группе будет удалено.

Пример

В данном примере показано, как настроить максимальное время ответа на интерфейсе. 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)#
```

51-10 ipv6 mld snooping query-version

Данная команда используется для того, чтобы настроить версию пакета General Query, отправленного MLD Snooping Querier. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ipv6 mld snooping query-version {1 | 2}
no ipv6 mld snooping query-version

Параметры

1	Укажите версию пакета MLD General Query, отправленного MLD Snooping Querier – 1.
2	Укажите версию пакета MLD General Query, отправленного MLD Snooping Querier – 2.

По умолчанию

Версия по умолчанию – 2.

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN.

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)#
```

51-11 ipv6 mld snooping report-suppression

Данная команда используется для включения функции MLD Report Suppression на VLAN. Используйте форму **no**, чтобы отключить MLD Report Suppression на VLAN.

ipv6 mld snooping report-suppression
no ipv6 mld snooping report-suppression

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. 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)#
```

51-12 ipv6 mld snooping robustness-variable

Данная команда используется для настройки значения robustness variable для MLD Snooping. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN.

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 интерфейсе VLAN 1000. Указанное значение – 3.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping robustness-variable 3
Switch(config-vlan)#
```

51-13 ipv6 mld snooping static-group

Данная команда используется для настройки статической группы MLD Snooping. Используйте форму **no**, чтобы удалить статическую группу.

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.
,	(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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Используйте данную команду на интерфейсе VLAN, чтобы статически добавить записи об участии в группе и/или записи источника (source).

Используйте команду **ipv6 mld snooping static-group,** чтобы создать статическую группу MLD Snooping, если прикрепленный узел не поддерживает протокол MLD.

Пример

В данном примере показано, как статически добавить группу и/или запись источника для MLD Snooping.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping static-group FF02::12:03 interface ethernet 1/0/5
Switch(config-vlan)#
```

51-14 ipv6 mld snooping suppression-time

Данная команда используется для того, чтобы настроить время блокирования дублированных сообщений MLD Report или MLD Leave. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ipv6 mld snooping suppression-time *SECONDS*
no ipv6 mld snooping suppression-time

Параметры

SECONDS	Укажите, чтобы настроить время блокирования дублированных сообщений MLD Report. Доступный диапазон значений: от 1 до 300.

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. 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)#
```

51-15 ipv6 mld snooping minimum-version

Данная команда используется для настройки минимальной версии MLD, разрешенной на интерфейсе. Используйте форму **no**, чтобы удалить заданное ограничение.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Данные настройки применимы только для фильтрации сообщений об участии MLD.

Пример

В данном примере показано, как ограничить подключение всех узлов MLDv1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping minimum-version 2
Switch(config-vlan)#
```

51-16 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, которую необходимо отобразить.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Если не указаны дополнительные параметры, 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       : v2
  Fast leave            : Enabled (host-based)
  Report suppression    : Enabled
  Suppression time      : 10 seconds
  Proxy reporting       : Disabled (Source ::)
  Mrouter port learning : Enabled
  Querier state         : Enabled (Non-active)
  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#
```

51-17 show ipv6 mld snooping groups

Данная команда используется для отображения информации о группе MLD Snooping, изученной на коммутаторе.

show ipv6 mld snooping groups [*IPV6-ADDRESS* **| vlan** *VLAN-ID***]**

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, который необходимо отобразить. Если VLAN не указана, будет отображена информация о группе MLD Snooping для всех VLAN.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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

MLD Snooping Connected Group Membership:

VLAN ID  Group address        Source address       FM  Exp(sec)  Interface
-------  -------------------  -------------------  --  --------  ---------
1        FF1E::                        *           EX  258       2/0/7
1        FF1E::3                       *           EX  258       2/0/7
1        FF1E::4              3620:110:1::3a2b     IN  258       2/0/7

Total Entries: 3

Switch#
```

Отображаемые параметры

FM	**Mode** (Режим фильтрации): Значение режима фильтрации может быть либо IN (Включить), либо EX (Исключить). EX - Режим фильтрации - Исключить. IN - Режим фильтрации - Включить.
Exp (sec)	**Expire time** (Время истечения): Время в секундах до истечения срока действия записи.

51-18 show ipv6 mld snooping mrouter

Данная команда используется для того, чтобы отобразить информацию 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, который необходимо отобразить. Если VLAN не указана, будет отображена информация о многоадресном маршрутизаторе MLD Snooping на всех VLAN.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить интерфейсы динамически изученного или сконфигурированного 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        1/0/3, 1/0/4  (static)
          1/0/6  (forbidden)
          1/0/7  (dynamic)

3        1/0/8  (static)
          1/0/9  (dynamic)

Total Entries: 2

Switch#
```

51-19 show ipv6 mld snooping static-group

Данная команда используется для отображения статически сконфигурированных групп MLD Snooping на коммутаторе.

show ipv6 mld snooping static-group [*GROUP-ADDRESS* **| vlan** *VLAN-ID***]**

Параметры

GROUP-ADDRESS	(Опционально) Укажите IPv6-адрес группы, который необходимо отобразить.
vlan *VLAN-ID*	(Опционально) Укажите VLAN ID, который необходимо отобразить.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Эта команда отображает информацию о статической группе MLD snooping.

Пример

В данном примере показано, как отобразить статически сконфигурированные группы MLD Snooping.

```
Switch#show ipv6 mld snooping static-group

VLAN ID  Group address                          Interface
-------  ---------------                        ------------------------
1        FF1E::1                                1/0/1,1/0/5

Total Entries: 1

Switch#
```

51-20 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, 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.
vlan	Укажите, чтобы отобразить счетчики статистики для VLAN.
VLAN-ID	(Опционально) Укажите VLAN ID, который необходимо отобразить.
,	(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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить статистику MLD Snooping.

Пример

В данном примере показано, как отобразить статистику MLD Snooping.

```
Switch# show ipv6 mld snooping statistics interface

Interface eth4/0/1
Rx: V1Report 1, v2Report 2, Query 1, v1Done 2
Tx: v1Report 1, v2Report 2, Query 1, v1Done 2

Interface eth4/0/3
Rx: V1Report 0, v2Report 0, Query 0, v1Done 0
Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Interface eth4/0/4
Rx: V1Report 3, v2Report 0, Query 3, v1Done 0
Tx: v1Report 2, v2Report 2, Query 1, v1Done 2

Total Entries: 3

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#
```

52. Команды Multiple Spanning Tree Protocol (MSTP)

52-1 instance

Данная команда используется для привязки VLAN к MST-экземпляру. Для удаления экземпляров без указания VLAN воспользуйтесь командой **no instance**. Для возврата привязки VLAN к экземпляру по умолчанию (CIST) воспользуйтесь командой **no instance**.

instance *INSTANCE-ID* **vlans** *VLAN-ID* **[, | -]**
no instance *INSTANCE-ID* **[vlans** *VLAN-ID* **[, | -]]**

Параметры

vlan *VLAN-ID*	Укажите VLAN, которые необходимо привязать или удалить из указанного экземпляра. Доступный 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.
INSTANCE-ID	Укажите ID MSTP-экземпляра, к которому необходимо привязать указанные VLAN. Доступный диапазон значений: от 1 до 4094.

По умолчанию

Нет

Режим ввода команды

MST Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

52-2 name

Данная команда используется для настройки имени MST-региона. Используйте форму no, чтобы вернуться к настройкам по умолчанию. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

name *NAME*
no name *NAME*

Параметры

NAME	Укажите имя MST-региона. Максимально допустимое количество символов – 32. Тип – общая строка, допускающая пробелы.

По умолчанию

Имя по умолчанию – MAC-адрес коммутатора.

Режим ввода команды

MST Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если у коммутаторов совпадают VLAN Mapping и номер версии конфигурации, но различаются имена регионов, они принадлежат к разным MST-регионам.

Пример

В данном примере показано, как настроить имя MSTP. Настроенное имя – MName.

```
Switch# configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)# name MName
Switch(config-mst)#
```

28-3 revision

Данная команда используется для настройки номера ревизии для MST. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

revision *VERSION*
no revision

Параметры

VERSION	Укажите номер ревизии для MST. Доступный диапазон значений: от 0 до 65535.

По умолчанию

Значение по умолчанию – 0.

Режим ввода команды

MST Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Два коммутатора Ethernet с идентичной конфигурацией принадлежат к разным регионам, если их номера ревизии не совпадают.

Пример

В данном примере показано, как настроить revision level MSTP. Настроенное значение – 2.

```
Switch# configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)# revision 2
Switch(config-mst)#
```

28-4 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	Укажите, чтобы отобразить таблицу соотношений между несколькими VLAN и экземплярами MSTP.
digest	(Опционально) Укажите для отображения дайджеста MD5, включенного в текущий идентификатор конфигурации MST (MSTCI).
instance *INSTANCE-ID* **[,	-]**	Укажите, чтобы отобразить информацию MSTP только для назначенного экземпляра. Отделите несколько экземпляров, используя «,», для перечисления нескольких экземпляров или отделения диапазона экземпляров от предыдущего. Используйте «-», для обозначения диапазона экземпляров. Пробелы до и после запятой и дефиса недопустимы.
interface *INTERFACE-*	Укажите, чтобы отобразить информацию STP для указанного интерфейса.

,	(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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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: 00-01-02-03-04-00, Priority: 32768 (32768 sysid 0)
 Designated Root Address: 00-00-00-00-00-00, Priority: 0 (0 sysid 0)
 Regional Root Bridge Address: 00-00-00-00-00-00, Priority: 0 (0 sysid 0)
 Designated Bridge Address: 00-00-00-00-00-00, Priority: 0 (0 sysid 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


Switch#
```

В данном примере показано, как отобразить подробную информацию об MSTP для интерфейса eth1/0/1.

```
Switch#show spanning-tree mst interface eth 1/0/1 detail

eth1/0/1
 Configured link type: auto, operation status: point-to-point
 Configured fast-forwarding: auto, operation status: non-edge

>>>>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.

```
Switch#show spanning-tree mst

 Spanning tree: Disabled,protocol: RSTP
 Number of MST instances: 1

>>>>MST00  vlans mapped : 1-4094
 Bridge Address: 00-01-02-03-04-00, Priority: 32768 (32768 sysid 0)
 Designated Root Address: 00-00-00-00-00-00, Priority: 0 (0 sysid 0)
 Regional Root Bridge Address: 00-00-00-00-00-00, Priority: 0 (0 sysid 0)
 Designated Bridge Address: 00-00-00-00-00-00, Priority: 0 (0 sysid 0)

                                              Priority
 Interface      Role       State      Cost      .Port#
 ---------      ----       -----      ----      -------
 eth1/0/1       nonStp     forwarding 200000    128.1


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 eth 1/0/3-4

eth1/0/3
Configured link type: auto, operation status: point-to-point
  Configured fast-forwarding: auto, operation status: edge

                                      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

                                      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 eth 1/0/3-4

>>>>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
                                         Priority
   Interface  Role       State      Cost    .Port#
---------  ----       -----      ------  ---------
eth1/0/3    backup     blocking   200000    128.3
eth1/0/4    backup     blocking   200000    128.4

Switch#
```

В данном примере показано, как отобразить настройки привязки экземпляра MSTP.

```
Switch# show spanning-tree mst configuration

Name     : [region1]
Revision : 2, Instances configured: 3
Digest   :  A222086F87562346CA7D40AD90AB61ED
Instance   Vlans
---------  -------------
0          21-4094
1          1-10
2          11-20

Switch#
```

28-5 spanning-tree mst

Данная команда используется для настройки параметров стоимости пути и приоритета порта для MST-экземпляра (включая CIST с ID экземпляра 0). Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

spanning-tree mst *INSTANCE-ID* **{cost** *COST* **| port-priority** *PRIORITY***}**
no spanning-tree mst *INSTANCE-ID* **{cost | port-priority}**

Параметры

instance *INTANCE-ID*	Укажите номер экземпляра.
cost *COST*	Укажите стоимость пути экземпляра. Доступный диапазон значений: от 0 до 200000000.
port-priority *PRIORITY*	Укажите приоритет порта экземпляра. диапазон значений: от 0 до 240 с шагом 16.

По умолчанию

Стоимость зависит от скорости порта. Чем выше скорость интерфейса, тем меньше стоимость. MST всегда использует стоимость длинного пути.

Приоритет порта по умолчанию – 128.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

При вводе стоимости запятая в записи не ставится. Например, 1000, а не 1,000.

Пример

В данном примере показано, как настроить стоимость пути интерфейса.

```
Switch# configure terminal
Switch(config)#interface eth 1/0/1
Switch(config-if)# spanning-tree mst 0 cost 17031970
Switch(config-if)#
```

28-6 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для входа в режим MST Configuration.

Пример

В данном примере показано, как войти в режим MST Configuration.

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

28-7 spanning-tree mst max-hops

Данная команда используется для настройки максимального числа переходов MSTP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

spanning-tree mst max-hops *HOP-COUNT*
no spanning-tree mst max-hops

Параметры

max-hops *HOP-COUNT*	Укажите максимальное число переходов MSTP. Доступный диапазон значений: от 1 до 40.

По умолчанию

Значение по умолчанию – 20 переходов.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить максимальное число переходов MSTP.

Пример

В данном примере показано, как настроить максимальное число переходов MSTP.

```
Switch# configure terminal
Switch(config)#spanning-tree mst max-hops 19
Switch(config)#
```

28-8 spanning-tree mst hello-time

Данная команда используется для настройки параметра Hello Time в версии MSTP для каждого порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

spanning-tree mst hello-time *SECONDS*
no spanning-tree mst hello-time

Параметры

SECONDS	Укажите интервал между отправкой одного BDPU-сообщения для назначенного порта (Designated Port). Доступный диапазон значений: от 1 до 2 секунд.

По умолчанию

Значение параметра Hello Time по умолчанию – 2 секунды.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12
Использование команды

Команда применима только в режиме MSTP.

Пример

В данном примере показано, как настроить параметр Hello Time в версии MSTP для интерфейса Ethernet 1/0/1. Указанное значение – 1 секунда.

```
Switch# configure terminal
Switch(config)#interface eth 1/0/1
Switch(config-if)# spanning-tree mst hello-time 1
Switch(config-if)#
```

28-9 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 ID MSTP-экземпляра. По умолчанию значение экземпляра CIST равно 0.
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

Уровень команды по умолчанию

Уровень 12

Использование команды

Приоритет имеет то же значение, что и приоритет моста в справочнике команд STP, но может указывать другой приоритет для разных MSTP-экземпляров.

Пример

В данном примере показано, как настроить приоритет моста для MSTP-экземпляра 2.

```
Switch# configure terminal
Switch(config)#spanning-tree mst 2 priority 0
Switch(config)#
```

53. Команды Neighbor Discovery (ND) Inspection

53-1 ipv6 nd inspection policy

Данная команда используется для создания политики ND Inspection Policy и для входа в режим ND Inspection Policy Configuration Mode. Используйте форму **no**, чтобы удалить политику ND Inspection Policy.

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

Уровень команды по умолчанию

Уровень 12

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)#
```

53-2 validate source-mac

Данная команда используется для проверки MAC-адреса на соответствие адресу Link Layer для ND-сообщений. Используйте форму **no**, чтобы отменить проверку.

validate source-mac
no validate source-mac

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

ND Inspection Policy Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Когда коммутатор получит 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)#
```

53-3 device-role

Данная команда используется для указания роли подключенного устройства. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

device-role {host | router}
no device-role

Параметры

host	Укажите, чтобы настроить устройство в качестве узла (Host).
router	Укажите, чтобы настроить устройство в качестве маршрутизатора (Router).

По умолчанию

Роль устройства по умолчанию – Host.

Режим ввода команды

ND Inspection Policy Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

53-4 ipv6 nd inspection attach-policy

Данная команда используется для применения политики ND Inspection Policy на определенном интерфейсе. Используйте форму **no**, чтобы удалить политику ND Inspection Policy.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки физического порта и port-channel. Используйте данную команду, чтобы применить политику ND Inspection Policy на определенном интерфейсе. Если указано **no policy-name**, 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 ethernet 1/0/3
Switch(config-if)# ipv6 nd inspection attach-policy policy1
Switch(config-if)#
```

53-5 show ipv6 nd inspection policy

Эта команда используется для отображения информации о политике защиты Router Advertisement (RA).

show ipv6 nd inspection policy [*POLICY-NAME***]**

Параметры

POLICY-NAME	(Необязательно) Укажите имя политики защиты IPv6 RA guard.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Если имя политики указано, отображаться будет информация только для указанной политики. Если имя политики не указано, отображаться будет информация для всех политик.

Пример

В этом примере показано, как отобразить конфигурацию политики для политики с 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#
```

54. Команды Network Access Authentication

54-1 authentication command bounce-port ignore

Эта команда используется для игнорирования команды RADIUS CoA bounce port. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

authentication command bounce-port ignore
no authentication command bounce-port ignore

Параметры

Нет

По умолчанию

По умолчанию принимается команда RADIUS CoA bounce port.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте эту команду для игнорирования или принятия команды RADIUS CoA bounce port. Команда RADIUS CoA bounce port, отправленная клиентом динамической авторизации, может вызвать сбой соединения на порту аутентификации.

Пример

В этом примере показано, как игнорировать команду RADIUS CoA bounce port.

```
Switch# configure terminal
Switch(config)# authentication command bounce-port ignore
Switch(config)#
```

54-2 authentication command disable-port ignore

Эта команда используется для игнорирования команды RADIUS CoA disable port. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

authentication command disable-port ignore
no authentication command disable-port ignore

Параметры

Нет

По умолчанию

По умолчанию команда RADIUS CoA disable port принимается.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте эту команду для игнорирования или принятия команды RADIUS CoA disable port. Команда RADIUS CoA disable port, отправленная от клиента динамической авторизации, может отключить порт аутентификации и завершить сеансы хостов на этом порту.

Пример

В этом примере показано, как игнорировать команду RADIUS CoA disable port.

```
Switch# configure terminal
Switch(config)# authentication command disable-port ignore
Switch(config)#
```

54-3 authentication guest-vlan

Эта команда используется для настройки параметров гостевой сети VLAN. Используйте форму **no** этой команды, чтобы удалить гостевую виртуальную локальную сеть.

authentication guest-vlan *VLAN-ID*
no authentication guest-vlan

Параметры

VLAN-ID	Укажите гостевую VLAN аутентификации.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда не может быть настроена, если указанная VLAN не существует как статическая VLAN. Хост не может получить доступ к сети, пока не пройдет аутентификацию. Если настроена гостевая VLAN, хосту разрешается доступ к гостевой VLAN без прохождения аутентификации. Во время аутентификации, если сервер RADIUS назначает пользователю VLAN, то пользователь будет авторизован в этой назначенной VLAN. Гостевая VLAN и назначение VLAN не действует на магистральном порту VLAN и туннельном порту VLAN. Обычно гостевая VLAN и назначение VLAN работают для хостов, которые подключаются к нетегированным портам. Это может вызвать неожиданное поведение, если оно работает на хостах, которые отправляют тегированные пакеты.

Если режим хост-аутентификации установлен на **multi-host**, порт будет добавлен как порт-член гостевой VLAN, а PVID порта изменится на гостевую VLAN. Трафик, приходящий из гостевой VLAN, может быть передан независимо от того, прошла ли аутентификация. Трафик, приходящий из других VLAN, будет отбрасываться до тех пор, пока не пройдет аутентификацию. Когда один хост пройдет аутентификацию, порт покинет гостевую VLAN и будет добавлен в назначенную VLAN. PVID порта будет изменен на назначенную VLAN.
Если режим хоста аутентификации установлен на **multi-auth**, порт будет добавлен как порт-член гостевой VLAN, а PVID порта будет изменен на гостевую VLAN. Хостам, которым разрешен доступ к гостевой VLAN, запрещен доступ к другим VLAN до тех пор, пока они не пройдут аутентификацию. Когда один хост пройдет аутентификацию, порт останется в гостевой VLAN, PVID порта не будет изменен.
Если гостевая VLAN отключена, порт выйдет из гостевой VLAN и вернется в родную VLAN. PVID изменится на родную VLAN.

Пример

В этом примере показано, как указать VLAN 5 в качестве гостевой VLAN.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# authentication guest-vlan 5
Switch(config-if)#
```

54-4 authentication host-mode

Эта команда используется для указания режима аутентификации. Используйте форму no этой команды, чтобы вернуться к настройкам по умолчанию.

authentication host-mode {multi-host | multi-auth [vlan *VLAN-ID* **[, | -]]}**
no authentication host-mode [multi-auth vlan *VLAN-ID* **[, | -]]**

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.
vlan *VLAN-ID*	(Опционально) Укажите VLAN аутентификации. Это может быть полезно, если различные VLAN на коммутаторе имеют различные требования к аутентификации. При использовании формы no все VLAN будут удалены, если не указаны конкретные. Это значит, что не важно, из какой VLAN клиент, клиент будет аутентифицирован, если MAC-

	адрес клиента (независимо от VLAN) не аутентифицирован. После аутентификации клиенту не нужно будет проходить повторную аутентификацию из других VLAN. Данная опция полезна для управления аутентификацией per-VLAN для портов trunk. Если режим аутентификации порта меняется на multi-host, предыдущие VLAN аутентификации на этом порту будут удалены.
,	(Опционально) Выделение серии или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию используется **multi-auth.**

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 заблокирован 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 порта Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication host-mode multi-host
Switch(config-if)#
```

54-5 authentication periodic

Данная команда используется для включения периодического повторения аутентификации для порта. При использовании формы **no** команда отключит периодическое повторение аутентификации.

authentication periodic
no authentication periodic

Параметры

Нет

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду для включения периодического повторения аутентификации для порта. Используйте команду **authentication timer reauthentication** для настройки таймера повторной аутентификации (re-authentication timer).

Пример

В данном примере показано, как включить периодическое повторение аутентификации для порта Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication periodic
Switch(config-if)#
```

54-6 authentication timer inactivity

Данная команда используется для настройки таймера бездействия, по истечении которого неактивная сессия будет завершена. При использовании формы **no** команда отключит таймер бездействия.

authentication timer inactivity {*SECONDS***}**
no authentication timer inactivity

Параметры

SECONDS	Укажите время, после которого неактивная сессия будет завершена. Доступен диапазон значений от 120 до 65535.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если таймер бездействия настроен, сессия пользователя будет завершена, если сеанс не будет работать в течение настроенного периода времени. Таймер бездействия (inactivity timer) должен быть меньше, чем значение таймера, настроенного с помощью команды **authentication timer reauthentication**.

Пример

В данном примере показано, как настроить значение таймера бездействия 240 для Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication timer inactivity 240
Switch(config-if)#
```

54-7 authentication timer reauthentication

Данная команда используется для настройки таймера, по истечении которого будет необходимо пройти повторную аутентификацию. При использовании формы **no** команда вернется к значениям по умолчанию.

authentication timer reauthentication {*SECONDS***}**
no authentication timer reauthentication

Параметры

SECONDS	Укажите время, после которого будет необходимо пройти повторную аутентификацию. Доступен диапазон значений от 1 до 65535.

По умолчанию

По умолчанию используется значение 3600 секунд.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для настройки таймера повторной аутентификации.

Пример

В данном примере показано, как настроить значение таймера повторной аутентификации 200 для Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication timer reauthentication 200
Switch(config-if)#
```

54-8 authentication timer restart

Данная команда используется для настройки таймера, по истечении которого станет возможна повторная аутентификация после последней неудачной попытки. При использовании формы **no** команда вернется к значениям по умолчанию.

authentication timer restart *SECONDS*
no authentication timer restart

Параметры

SECONDS	Указывает значение таймера перезапуска аутентификации. Диапазон составляет от 1 до 65535.

По умолчанию

По умолчанию используется значение 60 секунд.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Коммутатор будет в режиме молчания (Quiet State) после неудачной попытки аутентификации до истечения времени таймера.

Пример

В данном примере показано, как настроить значение таймера повторной аутентификации 20 для Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication timer restart 20
Switch(config-if)#
```

54-9 authentication username

Данная команда используется для создания пользователя в локальной базе данных аутентификации. При использовании формы **no** команда удалит пользователя из локальной базы данных аутентификации.

authentication username *NAME* **password [0 | 7]** *PASSWORD* **[vlan** *VLAN-ID***]**
no authentication username *NAME* **[vlan]**

Параметры

NAME	Укажите имя пользователя, состоящее не более чем из 32 символов.
0	(Опционально) Пароль в обычном текстовом виде. Если не указан ни 0, ни 7, по умолчанию паролем будет обычный текст.
7	(Опционально) Зашифрованный пароль. Если не указан ни 0, ни 7, по умолчанию паролем будет обычный текст.
password *PASSWORD*	Укажите, чтобы задать пароль для MAC-аутентификации. Если указан пароль в обычном текстовом виде, длина строки не может превышать 32 символа.
vlan *VLAN-ID*	(Опционально) Укажите, чтобы назначить VLAN.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Данная команда используется для настройки локальной базы 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)#
```

54-10 clear authentication sessions

Данная команда используется для удаления сессий аутентификации.

clear authentication sessions {mac | wac | dot1x | all | interface *INTERFACE-ID* **[mac | wac |dot1x] | mac-address** *MAC ADDRESS***}**

Параметры

mac	Укажите для удаления всех MAC-сессий.
wac	Укажите для удаления всех WAC-сессий.
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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для удаления сессий аутентификации.

Пример

В данном примере показано, как удалить сессии аутентификации на Ethernet 1/0/1.

```
Switch# clear authentication sessions interface ethernet 1/0/1
Switch#
```

54-11 authentication username mac-format

Данная команда используется для настройки формата MAC-адреса, который будет использоваться при аутентификации через RADIUS-сервер в качестве имени пользователя. При использовании формы **no** команда вернется к значениям по умолчанию.

authentication username mac-format case {lowercase | uppercase} delimiter {hyphen | colon |dot | none} number {1 | 2 | 5}

no authentication username mac-format

Параметры

lowercase	При аутентификации RADIUS формат имени пользователя будет выглядеть следующим образом: aa-bb-cc-dd-ee-ff
uppercase	При аутентификации RADIUS формат имени пользователя будет выглядеть следующим образом: AA-BB-CC-DD-EE-FF
hyphen	Укажите, чтобы использовать «-» в качестве разделителя. Формат будет выглядеть следующим образом: AA-BB-CC-DD-EE-FF
colon	Укажите, чтобы использовать «:» в качестве разделителя. Формат будет выглядеть следующим образом: AA:BB:CC:DD:EE:FF
dot	Укажите, чтобы использовать «.» в качестве разделителя. Формат будет выглядеть следующим образом:

	AA.BB.CC.DD.EE.FF
none	Укажите, чтобы не использовать знак разделения. Формат будет выглядеть следующим образом: AABBCCDDEEFF
number	Укажите количество знаков разделения. Доступны следующие опции: **1:** один разделитель; формат: AABBCC.DDEEFF **2:** два разделителя; формат: AABB.CCDD.EEFF **5:** пять разделителей; формат: AA.BB.CC.DD.EE.FF Если выбран параметр none, знаки разделения ограничителей не будут использоваться.

По умолчанию

По умолчанию для MAC-адреса аутентификации используются большие буквы.
По умолчанию знаком разделения MAC-адреса аутентификации является точка.
По умолчанию используется два знака разделения MAC-адреса аутентификации.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для настройки формата имени пользователя на основе MAC-адреса, используемого при аутентификации RADIUS или для IGMP Security.

Пример

В данном примере показано, как настроить формат имени пользователя на основе MAC-адреса.

```
Switch# configure terminal
Switch(config)# authentication username mac-format case uppercase delimiter hyphen number 5
Switch(config)#
```

54-12 authentication compauth mode

Данная команда используется для указания режима Compound Authentication Mode. При использовании формы **no** команда вернется к значениям по умолчанию.

authentication compauth mode {any | mac-jwac | mac-wac}
no authentication compauth mode

Параметры

any	Укажите для допуска, если допущен любой из методов аутентификации (802.1X, MAC-based Access Control и WAC). Если данный параметр используется, но MAC-based Access Control отключено, а 802.1X включено, то все равно будет

	необходима аутентификация 802.1X.
mac-jwac	Указывает, что сначала проверяется аутентификация на основе MAC. Если клиент проходит проверку, JWAC будет проверен следующим. Оба метода аутентификации должны быть пройдены.
mac-wac	Указывает, что сначала проверяется аутентификация на основе MAC. Если клиент проходит проверку, WAC будет проверен следующим. Оба метода аутентификации должны быть пройдены.

По умолчанию

По умолчанию используется опция **any**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда доступна только для конфигурации интерфейса физического порта. Используйте эту команду для настройки метода аутентификации на портах.

Настройка включения или отключения индивидуальной аутентификации будет действовать всегда. Если метод индивидуальной аутентификации на порту установлен на любой, но отключен контроль доступа на основе MAC, а JWAC и 802.1X включены, то пользователь должен пройти либо метод JWAC, либо 802.1X. Если метод **mac-jwac** или **mac-wac**, пользователь авторизуется после прохождения двух методов аутентификации. Если ни один из методов не прошел, пользователю будет отказано. Если глобальное состояние соответствующего метода или состояние порта не включено, пользователь отклоняется (из-за отсутствия аутентификации). После аутентификации авторизованная информация будет получена из модуля JWAC или WAC.

Пример

В данном примере показано, как настроить режим **mac-wac** для Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#authentication compauth mode mac-wac
Switch(config-if)#
```

54-13 authentication max users

Данная команда используется для настройки максимального количества аутентифицированных пользователей для всей системы или для порта. При использовании формы **no** команда вернется к значениям по умолчанию.

authentication max users *NUMBER*
no authentication max users

Параметры

NUMBER	Указывает для установки максимального числа аутентифицированных пользователей. Диапазон составляет от 1 до 1000.

По умолчанию

По умолчанию ограничений нет.

Режим ввода команды

Global Configuration Mode
Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда может использоваться 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, MAC-based Access Control и WAC.

Также команда имеет следующее ограничение:

- 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)#
```

54-14 authentication mac-move deny

Эта команда используется для отключения MAC-перемещения на коммутаторе. Используйте форму **no** этой команды, чтобы возврата к настройкам по умолчанию.

authentication mac-move deny
no authentication mac-move deny

Параметры

Нет

По умолчанию

По умолчанию этот параметр разрешен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда определяет, разрешать ли аутентифицированным хостам перемещаться по разным портам коммутатора. Эта команда управляет только тем, разрешено ли хосту, который аутентифицирован на порту, установленном в режим **multi-auth**, перемещаться на другой порт.

Если станции разрешено перемещение, возможны две ситуации. Ей может потребоваться повторная аутентификация или прямое перемещение на новый порт без повторной аутентификации на основании следующего правила. Если новый порт имеет ту же конфигурацию аутентификации, что и исходный порт, то повторная аутентификация не требуется. Хост унаследует те же атрибуты авторизации с новым портом. Аутентифицированный хост может перемещаться с порта 1 на порт 2 и наследовать атрибуты авторизации без повторной аутентификации. Если новый порт имеет другую конфигурацию аутентификации, чем исходный порт, то необходима повторная аутентификация. Аутентифицированный хост на порту 1 может переместиться и повторно аутентифицироваться на порту 2. Если на новом порту не включен метод аутентификации, то станция напрямую перемещается на новый порт. Сессия с исходным портом удаляется. Аутентифицированный узел на порту 1 может быть перемещен на порт 2.

Если MAC move отключен и аутентифицированный хост переходит на другой порт, то это рассматривается как ошибка нарушения.

Пример

В этом примере показано, как включить перемещение MAC-адресов на коммутаторе.

```
Switch# configure terminal
Switch(config)# authentication mac-move deny
Switch(config)#
```

54-15 authorization disable

Данная команда используется для отключения приема авторизованной конфигурации. При использовании формы **no** команда включит принятие авторизованной конфигурации.

authorization disable
no authorization disable

Параметры

Нет

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для включения или отключения приема авторизованной конфигурации. Когда авторизация включена для аутентификации, авторизованные атрибуты (например, VLAN, приоритет 802.1p по умолчанию, пропускная способность и ACL), назначенные сервером RADIUS, будут приняты, если статус авторизации включен. Полоса пропускания и ACL назначаются на основе каждого порта. Если в режиме **multi-auth**, VLAN и 802.1p назначаются на основе каждого хоста. В противном случае пропускная способность и ACL назначаются на основе каждого порта.

Пример

В этом примере показано, как включить статус авторизации.

```
Switch# configure terminal
Switch(config)# no authorization disable
Switch(config)#
```

54-16 show authentication sessions

Данная команда используется для просмотра информации об аутентификации.

show authentication sessions [mac | wac | jwac| dot1x | interface *INTERFACE-ID* **[, | -] [mac | wac | dot1x] | mac-address** *MAC-ADDRESS***]**

Параметры

mac	(Опционально) Укажите для отображения всех MAC-сессий.
wac	(Опционально) Укажите для отображения всех WAC-сессий.
jwac	(Опционально) Указывает отображение всех сеансов JWAC.
dot1x	(Опционально) Укажите для отображения всех сессий dot1x.
interface *INTERFACE-ID*	(Опционально) Укажите порт для отображения.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
mac-address *MAC-ADDRESS*	(Опционально) Укажите для отображения определенного

пользователя.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте команду без параметров, чтобы включить отображение сессий со всех портов.

Пример

В данном примере показано, как включить отображение сессий на Ethernet 1/0/1.

```
Switch# show authentication sessions interface eth1/0/1

Interface: eth1/0/1
MAC Address: 00-40-10-28-19-78
Authentication VLAN: 100
Authentication State: Success
Accounting Session ID: 100000000003
Assigned Ingress Bandwidth: 500000 kbps
Assigned Egress Bandwidth: 1000000 kbps
Assigned User ACL:
 ip access-list extended radius-deny-telnet;deny tcp any any eq telnet;exit;
 ip access-list standard 1;10 deny tcp any any eq telnet;exit;
Aging Time: 3600 sec
Methods State
  802.1X: Failed
  802.1X Authenticator State: HELD
  802.1X Backend State: IDLE
  MAC-based Access Control: Success, Selected
  WEB-based Access Control: No Information

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
Accounting Session ID	ID сессии учетной записи, который использовался для учета после аутентификации.
Authentication Username	Имя пользователя узла. Недоступно, пока узел выбран для MAC-Auth.
Client IP Address	Адрес ассоциированных клиентов. Доступен, только если узел выбран для Web-Auth.
Assigned VID	Назначенный VLAN ID, разрешенный после прохождения узлом аутентификации.
Assigned Priority	Назначенный приоритет, разрешенный после прохождения узлом аутентификации.
Assigned Ingress Bandwidth	Назначенный вход, разрешенный после прохождения узлом аутентификации.
Assigned Egress Bandwidth	Назначенный выход, разрешенный после прохождения узлом аутентификации.
Method	Метод аутентификации, например, 802.1X, MAC-Auth, Web-Auth и т.д.
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.
Aging Time/Block Time	**Aging Time** – время старения, период времени, во время которого аутентифицированный узел будет сохраняться в аутентифицированном состоянии. По истечении данного времени узел будет возвращен 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.
Idle Time	Оставшееся время сессии аутентификации, которое будет завершено, если сессия неактивна в течение настроенного

	периода времени. Доступно только для сессий WEB.
802.1X Authenticator State	Состояние аутентификатора PAE 802.1X: возможны следующие значения: **INITIALIZE** – аутентификатор в процессе инициализации и ожидает запросы 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 подключиться к запрашивающему устройству. **AUTHENTICATING** – запрашивающее устройство проходит аутентификацию. **AUTHENTICATED** – аутентификатор успешно аутентифицировал запрашивающее устройство. **ABORTING** – процедура аутентификации преждевременно отменена из-за запроса на повторную авторизацию или запроса кадра EAPOL- Start, EAPOL-Logoff, тайм-аута 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.

55. Команды Network Protocol Port Protection

55-1 network-protocol-port protect

Эта команда используется для включения функции защиты порта сетевого протокола. Используйте форму **no** этой команды для отключения этой функции.

network-protocol-port protect {tcp | udp}
no network-protocol-port protect {tcp | udp}

Параметры

tcp	Указывает на защиту порта TCP.
udp	Указывает для защиты порт UDP.

По умолчанию

По умолчанию эта функция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для включения или отключения функции защиты порта сетевого протокола. Если порт защищен, коммутатор не будет отправлять ответные пакеты на закрытый порт TCP или UDP.

Пример

В этом примере показано, как включить защиту портов TCP.

```
Switch#configure terminal
Switch(config)#network-protocol-port protect tcp
Switch(config)#
```

55-2 show network-protocol-port protect

Эта команда используется для отображения информации о защите порта сетевого протокола.

show network-protocol-port protect

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду 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#
```

56. Команды Network Time Protocol (NTP)

56-1 ntp access-group

Данная команда используется для управления службами NTP на коммутаторе. Используйте форму **no**, чтобы отменить управление доступом служб NTP.

ntp access-group {default | *IP-ADDRESS* **[***IP-MASK***] |** *IPV6-ADDRESS* **|** *IPV6-ADDRESS* **/** *PREFIX-LENGTH***} [ignore] [nomodify] [noquery] [nopeer] [noserve] [notrust] [version]**

no ntp access-group {default | *IP-ADDRESS* **[***IP-MASK***] |** *IPV6-ADDRESS* **|** *IPV6-ADDRESS* **/** *PREFIX-LENGTH***}**

Параметры

default	Укажите, чтобы использовать IPv4-адрес (0.0.0.0/0.0.0.0) или IPv6-адрес (::/::) address по умолчанию. У IP-адреса по умолчанию всегда самый низкий приоритет в списке.
IP-ADDRESS	Укажите IP-адрес узла или сети.
IP-MASK	(Опционально) Укажите маску IP-адреса.
IPV6-ADDRESS	Укажите IPv6-адрес узла или сети.
IPV6-ADDRESS **/** *PREFIX-LENGTH*	(Опционально) Укажите длину префикса IPv6.
ignore	(Опционально) Укажите, чтобы запретить доступ всем пакетам, включая NTP Control Queries.
nomodify	(Опционально) Укажите, чтобы запретить доступ NTP Control Queries, которые пытаются изменить состояние сервера.
noquery	(Опционально) Укажите, чтобы запретить доступ всем NTP Control Queries.
nopeer	(Опционально) Укажите, чтобы запретить доступ пакетам, которые могут быть ассоциированы без аутентификации. Пакеты могут быть: Broadcast, Symmetric-active и Manycast. Обратите внимание, что данный параметр применяется только к пакетам, которые могут быть ассоциированы.
noserve	(Опционально) Укажите, чтобы запретить доступ всем пакетам, кроме NTP Control Queries.
notrust	(Опционально) Укажите, чтобы запретить доступ пакетам, которые не прошли криптографическую аутентификацию. Если команда **ntp authenticate** включена, аутентификация проводится для всех пакетов, которые могут запустить ассоциацию. Если команда **ntp authenticate** отключена, но не присутствует параметр notrust, ассоциация может быть запущена независимо от того, аутентифицирован пакет или нет. Если команда **ntp authenticate** отключена, но параметр notrust указан, аутентификация требуется только для указанного диапазона адресов/масок.
version	(Опционально) Укажите, чтобы запретить доступ пакетам, не соответствующим текущей NTP-версии.

По умолчанию

По умолчанию все системы получают полный доступ, если указан только один параметр – **default**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

NTP реализует общее назначение списка управления доступом ACL (Access Control List), содержащего записи адресов/совпадений. Записи отсортированы по возрастанию значений адресов, а затем по возрастанию значений масок. Совпадение происходит, когда побитовое И (AND) маски и адреса источника пакета равно побитовому И (AND) маски и адреса в списке. Список просматривается по порядку и применяется политика последнего совпавшего правила.

Пример

В данном примере показано, как запретить новые ассоциации по умолчанию, кроме 192.43.244.18, 128.175.0.0/16 и 128.4.1.0/24, для которых требуется аутентификация.

```
Switch#configure terminal
Switch(config)#ntp access-group default nopeer
Switch(config)#ntp access-group 128.175.0.0
Switch(config)#ntp access-group 128.4.1.0 notrust
Switch(config)#ntp access-group 192.43.244.18
Switch(config)#
```

56-2 ntp authenticate

Данная команда используется для включения NTP-аутентификации. Используйте форму **no**, чтобыотключить NTP-аутентификацию.

ntp authenticate
no ntp authenticate

Параметры

Нет

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если NTP-аутентификация включена, сетевые узлы будут синхронизированы с коммутатором только при наличии ключа, указанного в команде **ntp trusted-key**.

Пример

В данном примере показано, как включить NTP-аутентификацию.

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

56-3 ntp authentication-key

Данная команда используется для добавления ключа аутентификации для NTP. Используйте форму **no**, чтобы удалить ключ.

ntp authentication-key *KEY-ID* **md5** *VALUE*
no ntp authentication-key *KEY-ID*

Параметры

KEY-ID	Укажите ID NTP-ключа. Доступный диапазон значений: от 1 до 255.
md5	Укажите тип MD5 для ключа аутентификации.
VALUE	Укажите ключевую строку. Максимально допустимое количество символов в строке – 32.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для добавления ключа аутентификации для NTP. Используйте форму **no**, чтобы удалить ключ.

Пример

В данном примере показано, как добавить ключ аутентификации. ID добавленного ключа – 45. Ключевая строка – NTPKey.

```
Switch#configure terminal
Switch(config)#ntp authentication-key 45 md5 NTPKey
Switch(config)#
```

56-4 ntp control-key

Данная команда используется для указания ID ключа для контрольных NTP-сообщений. Используйте форму **no**, чтобы удалить ключ.

ntp control-key *KEY-ID*
no ntp control-key

Параметры

KEY-ID	Укажите ID NTP-ключа. Доступный диапазон значений: от 1 до 255.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для указания ID ключа для контрольных NTP-сообщений.

Пример

В данном примере показано, как указать ID ключа для контрольных NTP-сообщений.

```
Switch#configure terminal
Switch(config)#ntp control-key 45
Switch(config)#
```

56-5 ntp disable

Данная команда используется для отключения отправки NTP-пакетов на интерфейсе. Используйте форму **no**, чтобы включить отправку NTP-пакетов на интерфейсе.

ntp disable
no ntp disable

Параметры

Нет

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для отключения/включения отправки NTP-пакетов на интерфейсе.

Пример

В данном примере показано, как отключить отправку NTP-пакетов на интерфейсе VLAN 1.

```
Switch# configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ntp disable
Switch(config-if)#
```

56-6 ntp master

Данная команда используется для настройки RTC в качестве основных NTP-часов, в случае если внешний NTP недоступен. Используйте форму **no**, чтобы отключить данную функцию.

ntp master *STRATUM*
no ntp master

Параметры

STRATUM	Укажите часовой слой NTP. Доступный диапазон значений: от 1 до 15.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки RTC в качестве основных NTP-часов, в случае если внешний NTP недоступен. Используйте форму no, чтобы отключить данную функцию.

Пример

В данном примере показано, как настроить маршрутизатор в качестве основных часов NTP.

```
Switch#configure terminal
Switch(config)#ntp master 10
Switch(config)#
```

56-7 ntp max-associations

Данная команда используется для настройки максимального количества NTP-узлов и клиентов на коммутаторе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ntp max-associations *NUMBER*
no ntp max-associations

Параметры

NUMBER	Укажите количество NTP-ассоциаций. Доступный диапазон значений: от 1 до 64.

По умолчанию

Значение по умолчанию – 32.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки максимального количества NTP-узлов и клиентов на коммутаторе.

Пример

В данном примере показано, как настроить максимальное количество NTP-ассоциаций, равное 20.

```
Switch#configure terminal
Switch(config)#ntp max-associations 20
Switch(config)#
```

56-8 ntp peer

Данная команда используется для настройки NTP-узлов. Используйте форму **no**, чтобы отключить данную функцию.

ntp peer {*IP-ADDRESS* **|** *IPv6-ADDRESS***} [version** *NUMBER***] [key** *KEY-ID***] [prefer] [min-poll** *INTERVAL***] [max-poll** *INTERVAL***]**
no ntp peer {*IP-ADDRESS* **|** *IPv6-ADDRESS***}**

Параметры

IP-ADDRESS	Укажите IPv4-адрес узла.
IPv6-ADDRESS	Укажите IPv6-адрес узла.
version	(Опционально) Укажите номер NTP-версии.
NUMBER	(Опционально) Введите номер NTP-версии. Доступный диапазон значений: от 1 до 4. Значение по умолчанию – 4.
key	(Опционально) Укажите ключ аутенификации.
KEY-ID	(Опционально) Укажите ID ключа аутентификации. Доступный диапазон значений: от 1 до 255.
prefer	(Опционально) Укажите предпочтительный для синхронизации узел.
min-poll	(Опционально) Укажите минимальный интервал опроса для NTP- сообщений. Интервал опроса рассчитывается как 2 в степени указанного значения. Например, если указано значение 6, то минимальный интервал опроса будет составлять 64 секунды (2^6=64).
INTERVAL	(Опционально) Укажите значение минимального интервала опроса. Значение по умолчанию – 6.
max-poll	(Опционально) Укажите максимальный интервал опроса для NTP- сообщений. Интервал опроса рассчитывается как 2 в степени указанного значения. Например, если указано значение 6, то максимальный интервал опроса будет составлять 64 секунды (26=64).
INTERVAL	(Опционально) Укажите значение максимального интервала опроса. Значение по умолчанию – 10.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Настройки NTP системного времени коммутатора могут быть синхронизированы с узлом.

Пример

В данном примере показано, как настроить IP-адрес 192.168.22.33 для NTP-узла с использованием NTP-версии 3.

```
Switch#configure terminal
Switch(config)#ntp peer 192.168.22.33 version 3
Switch(config)#
```

56-9 ntp request-key

Данная команда используется для указания ID ключа для NTP-пакетов Mode 7, используемых утилитой *ntpdc*. Используйте форму **no**, чтобы удалить ключ.

ntp request-key *KEY-ID*
no ntp request-key

Параметры

KEY-ID	Укажите ID NTP-ключа. Доступный диапазон значений: от 1 до 255.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Утилита *ntpdc* использует проприетарный протокол (Proprietary Protocol), указанный для реализации NTP.

Пример

В данном примере показано, как указать ключ NTP Request.

```
Switch#configure terminal
Switch(config)#ntp request-key 45
Switch(config)#
```

56-10 ntp server

Данная команда используется для синхронизации времени коммутатора с NTP-сервером. Используйте форму **no**, чтобы отключить данную функцию.

ntp server {*IP-ADDRESS* **|** *IPv6-ADDRESS***} [version** *NUMBER***] [key** *KEY-ID***] [prefer] [min-poll** *INTERVAL***] [max-poll** *INTERVAL***]**
no ntp server {*IP-ADDRESS* **|** *IPv6-ADDRESS***}**

Параметры

IP-ADDRESS	Укажите IPv4-адрес узла.

IPv6-ADDRESS	Укажите IPv6-адрес узла.
version	(Опционально) Укажите номер NTP-версии.
NUMBER	(Опционально) Введите номер NTP-версии. Доступный диапазон значений: от 1 до 4. Значение по умолчанию – 4.
key	(Опционально) Укажите ключ аутенификации.
KEY-ID	(Опционально) Укажите ID ключа аутентификации. Доступный диапазон значений: от 1 до 255.
prefer	(Опционально) Укажите предпочтительный для синхронизации узел.
min-poll	(Опционально) Укажите минимальный интервал опроса для NTP- сообщений. Интервал опроса рассчитывается как 2 в степени указанного значения. Например, если указано значение 6, то минимальный интервал опроса будет составлять 64 секунды (2^6=64).
INTERVAL	(Опционально) Укажите значение минимального интервала опроса. Значение по умолчанию – 6.
max-poll	(Опционально) Укажите максимальный интервал опроса для NTP- сообщений. Интервал опроса рассчитывается как 2 в степени указанного значения. Например, если указано значение 6, то максимальный интервал опроса будет составлять 64 секунды (26=64).
INTERVAL	(Опционально) Укажите значение максимального интервала опроса. Значение по умолчанию – 10.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для синхронизации времени коммутатора с NTP-сервером.

Пример

В данном примере показано, как настроить IP-адрес 192.168.10.33 для NTP-сервера с использованием NTP-версии 2.

```
Switch#configure terminal
Switch(config)#ntp server 192.168.10.33 version 2
Switch(config)#
```

56-11 ntp trusted-key

Данная команда используется для указания доверенного ключа узла, который будет аутентифицирован NTP-системой. Используйте форму **no**, чтобы отключить данную функцию.

ntp trusted-key *KEY-ID*
no ntp trusted-key *KEY-ID*

Параметры

KEY-ID	Укажите ID NTP-ключа. Доступный диапазон значений: от 1 до 255.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для указания доверенного ключа узла, который будет аутентифицирован NTP-системой. Используйте форму **no**, чтобы отключить данную функцию.

Пример

В данном примере показано, как настроить доверенный NTP-ключ.

```
Switch#configure terminal
Switch(config)#ntp trusted-key 45
Switch(config)#
```

56-12 ntp update-calendar

Данная команда используется для периодической синхронизации аппаратных часов со временем, полученным по NTP. Используйте форму **no**, чтобы отключить данную функцию.

ntp update-calendar
no ntp update-calendar

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для периодической синхронизации аппаратных часов со временем, полученным по NTP. Используйте форму **no**, чтобы отключить данную функцию.

Пример

В данном примере показано, как периодически синхронизировать аппаратные часы со временем, полученным по NTP.

```
Switch#configure terminal
Switch(config)#ntp update-calendar
Switch(config)#
```

56-13 service ntp

Данная команда используется для включения NTP. Используйте форму **no**, чтобы отключить данную функцию.

service ntp
no service ntp

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки общего состояния NTP.

Пример

В данном примере показано, как включить NTP.

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

56-14 show ntp associations

Данная команда используется для отображения статуса NTP-ассоциаций.

show ntp associations [detail]

Параметры

detail	(Опционально) Укажите для отображения подробной информации по каждой NTP-ассоциации.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения статуса NTP-ассоциаций.

Пример

В данном примере показано, как отобразить NTP-ассоциации.

```
Switch#show ntp associations

     Remote           Local      St Poll Reach  Delay   Offset    Disp
==============================================================================
-192.168.10.33   0.0.0.0         16  128    0 0.00000  0.000000 3.99217
+192.168.22.33   0.0.0.0         16  128    0 0.00000  0.000000 3.99217
+ Symmetric active, - Symmetric passive, = Client, * System Peer

Switch#
```

Отображаемые параметры

Leading Characters	Ниже перечислены возможные первые символы в строке, отображаемойна дисплее: **+** – Symmetric Active Mode **-** – Symmetric Passive Mode **=** – Client Mode **^** – Broadcast Mode

	~ – Broadcast Client ***** – System Peer
Remote	IP-адрес узла.
Local	IP-адрес локального интерфейса.
St	Часовой слой узла.
Poll	Интервал опроса в секундах.
Reach	Успешное достижение узла.
Delay	Задержка прохождения сигнала в прямом и обратном направлении к одноранговому узлу.
Offset	Относительное время узла по отношению к локальному времени в миллисекундах. (Положительное значение указывает, что показания часов сервера больше. Отрицательное значение указывает, что показания часов узла больше).
Disp	Дисперсия (Dispersion). Максимальная разница во времени, которая когда-либо наблюдалась между локальными часами и часами сервера.

В данном примере показано, как отобразить NTP-ассоциации подробно.

```
Switch# show ntp associations detail

Remote 192.168.10.33, Local 0.0.0.0
Our mode client, Peer mode unspec, Stratum 16, Precision -7
Leap 11, RefID [INIT], RootDistance 0.00000, RootDispersion 0.00000
PPoll 10, HPoll 10, KeyID 0, Version 2, Association 8356
Reach 000, Unreach 17, Flash 0x1400, Timer 840s, flags  Config
Reference Timestamp:  00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
Originate Timestamp: 00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
Receive Timestamp:   00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
Transmit Timestamp:  00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
Filter Delay:  0.00000  0.00000  0.00000  0.00000
               0.00000  0.00000  0.00000  0.00000
Filter Offset: 0.000000 0.000000 0.000000 0.000000
               0.000000 0.000000 0.000000 0.000000
Filter Order:  0        1        2        3
               4        5        6        7
Offset 0.000000, Delay 0.00000, Error Bound 3.99217, Filter Error 0.00000

Remote 192.168.22.33, Local 0.0.0.0
Our mode sym_active, Peer mode unspec, Stratum 16, Precision -7
Leap 11, RefID [INIT], RootDistance 0.00000, RootDispersion 0.00000
PPoll 10, HPoll 10, KeyID 0, Version 3, Association 8355
Reach 000, Unreach 17, Flash 0x1400, Timer 798s, flags  Config
Reference Timestamp:  00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Отображаемые параметры

Remote	IP-адрес узла.
Local	IP-адрес коммутатора.

Our mode	Наш режим по отношению к узлу. Доступные режимы: **active**, **passive**, **client**, **server**, **bdcast** и **bdcastclient**.
Peer mode	Режим узла по отношению к нам.
Stratum	Часовой слой узла.
Precision	Точность часов узла в Гц.
Leap	Leap-индикатор. Доступный диапазон значений: от 0 до 3.
RefID	IP-адрес узла устройства, с которым необходимо настроить синхронизацию.
RootDistance	Корневая задержка. Задержка в миллисекундах к корневому устройству настройки NTP.
RootDispersion	Корневая дисперсия. Максимальная разница во времени, которая когда- либо наблюдалась между локальными и корневыми часами.
PPoll	Экспонента опроса узла (Peer).
HPoll	Экспонента опроса хоста (Host).
KeyID	ID ключа аутентификации.
Version	NTP-версия, используемая узлом.
Association	ID ассоциации.
Reach	Успешное достижение узла.
Unreach	Счетчик неуспешных попыток достижения узла.
Flash	Необходима диагностика для выявления проблем.
Timer	Таймер узла в секундах.
Flags	Флаги узла.
Reference Timestamp	Время последней установки или корректировки системных часов.
Originate Timestamp	Время отправленного запроса клиента на сервер.
Receive Timestamp	Время полученного запроса клиента на сервер.
Transmit Timestamp	Время отправленного ответа сервера клиенту.
Filter Delay	Задержка приема/передачи (Round-Trip Delay) каждой выборки в миллисекундах.
Filter Offset	Сдвиг часов (Clock Offset) каждой выборки в миллисекундах.
Filter Order	Порядок фильтрации каждой выборки.
Offset	Сдвиг часов узла по отношению к нашему времени.
Delay	Задержка приема/передачи (Round-Trip Delay) для узла.
Error Bound	Дисперсия (Dispersion) узла.
Filter Error	Ошибка аппроксимации (Approximate Error) каждой выборки.
St	Часовой слой узла.
Poll	Интервал опроса в секундах.
Reach	Успешное достижение узла.
Delay	Задержка прохождения сигнала в прямом и обратном направлении к одноранговому узлу.
Offset	Относительное время узла по отношению к локальному времени в миллисекундах. (Положительное значение указывает, что показания часов сервера больше.

	Отрицательное значение указывает, что показания часов узла больше).
Disp	Дисперсия (Dispersion). Максимальная разница во времени, которая когда-либо наблюдалась между локальными часами и часами сервера.

56-15 show ntp status

Данная команда используется для отображения статуса функции NTP.

show ntp status

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения статуса функции NTP.

Пример

В данном примере показано, как отобразить статус функции NTP.

```
Switch# show ntp status

Leap Indicator:       Unsynchronized
Stratum:              16
Precision:            -8
Root Distance:        0.00000 s
Root Dispersion:      0.10680 s
Reference ID:         [INIT]
Reference Time:       00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
System Flags:         Auth Monitor NTP Kernel Stats
Jitter:               0.000000 s
Stability:            0.000 ppm
Auth Delay:           0.000000 s

Switch#
```

Отображаемые параметры

Remote	IP-адрес узла.
Local	IP-адрес коммутатора.
Our mode	Наш режим по отношению к узлу. Доступные режимы: **active**, **passive**, **client**, **server**, **bdcast** и **bdcastclient**.
Peer mode	Режим узла по отношению к нам.
Leap Indicator	**Synchronized** – коммутатор синхронизирован с NTP-узлом. **Unsynchronized** – коммутатор не синхронизирован с NTP-узлом.
Stratum	Часовой слой коммутатора.
Precision	Точное значение.
RootDistance	Корневая задержка. Задержка в миллисекундах к корневому устройству настройки NTP.
RootDispersion	Корневая дисперсия. Максимальная разница во времени, которая когда-либо наблюдалась между локальными и корневыми часами.
Reference ID	IP-адрес узла устройства, с которым необходимо настроить синхронизацию.
Reference Time	Эталонная временная метка (Reference Timestamp).
System Flags	**Auth** – необходимо настроить аутентификацию. **Monitor** – включение монитора. **NTP** – функция NTP включена. **Kernel** – поддержка ядра включена. **Stats** – контроль статуса системы.
Jitter	Джиттер системы.
Stability	Стабильность частоты (Wander) (s/s).
Auth Delay	Задержка аутентификации.

57. Команды Port Security

57-1 clear port-security

Данная команда позволяет удалить динамически изученные безопасные MAC-адреса.

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) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда позволяет 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#
```

57-2 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, который необходимо отобразить.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Команда используется для отображения текущих настроек Port Security.

Пример

В данном примере показано, как включить отображение настроек Port Security для Ethernet с 1/0/1 по 1/0/3.

```
Switch#show port-security interface ethernet 1/0/1-3

 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#
```

57-3 snmp-server enable traps port-security

Данная команда используется для включения отправки SNMP-уведомлений при обнаружении функционалом Port Security недопустимых адресов. При использовании формы **no** команда отключит отправку SNMP-уведомлений.

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 трапов в секунду. Доступен 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для включения или отключения отправки SNMP-уведомлений при обнаружении функционалом Port Security недопустимых адресов.

Пример

В данном примере показано, как включить отправку трапов при обнаружении функционалом Port Security недопустимых адресов и установить количество трапов в секунду, равное 3.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps port-security trap-rate 3
Switch(config)#
```

57-4 switchport port-security

Данная команда используется для настройки параметров Port Security, чтобы ограничить количество пользователей, которым разрешен доступ к порту. Используйте форму **no** этой команды для отключения Port Security или удаления безопасного MAC-адреса.

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. Доступен диапазон значений от 0 до 6656.
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 (system log).
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

Уровень команды по умолчанию

Уровень 12

Использование команды

Когда включена функция Port Security, если режим порта port mode настроен как **delete-on-timeout**, порт автоматически будет изучать безопасные записи и хранить их, пока не истечет их время тайм- аута. 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 состояния безопасности режима порта (port mode-security) счетчик нарушений будет сброшен, записи Auto-permanent будут преобразованы в соответствующие динамические записи. При отключении режима порта port-security автоматически изученные безопасные записи будут удалены, включая динамические и постоянные (Permanent), а также счетчик нарушений. При изменении настройки VLAN автоматически изученные динамические безопасные записи будут удалены.

Постоянные безопасные записи будут храниться в текущем файле конфигурации (running configuration) и могут быть сохранены в NVRAM при использовании команды **copy**. Настроенные пользователем безопасные MAC-адреса будут подсчитываться в максимальном количестве MAC- адресов на порт.

Так как постоянная (permanent) безопасная запись Port Security включена на порту, MAC-адрес нельзя перенести на другой порт.

При изменении настроек изученные адреса останутся неизменными, если максимальное число будет увеличено. Если максимальное число будет изменено на меньшее, чем существующее число изучаемых записей, команда будет отклонена.

Порт с поддержкой Port Security имеет следующие ограничения:

- Функция Port Security не может функционировать одновременно с 802.1X, MAC-based Access Control (управление доступом на основе MAC), WAC 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, и возрастает счетчик нарушений безопасности.
- **Shutdown** – при нарушении безопасности интерфейс отключается на основе ошибок.

Пример

В данном примере показано, как настроить режим permanent для Port Security 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 данном примере показано, как вручную добавить безопасный MAC-адрес 00-00-12-34-56-78 с VID 5 на 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 данном 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)#
```

57-5 switchport port-security aging

Данная команда позволяет задать время старения (aging time) для динамически изученных безопасных адресов на интерфейсе. При использовании формы **no** команда вернется к значениям по умолчанию.

switchport port-security aging {time *MINUTES* **| type {absolute | inactivity}}**
no switchport port-security aging {time | type}

Параметры

time *MINUTES*	Укажите время старения (aging time) для динамически изученных безопасных адресов на порту в минутах. Доступен диапазонзначений от 0 до 1440.
type	Укажите тип старения.
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

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для отключения процесса старения записей, а также для того, чтобы задать время старения динамически изученных безопасных записей. Для того чтобы задать тип **inactivity**, должна быть включена функция FDB Table Ageing.

Пример

В данном примере показано, как настроить время старения динамически изученных безопасных MAC-адресов для Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security aging 1
Switch(config-if)#
```

В данном примере показано, как настроить тип времени старения для Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)#
```

57-6 port-security limit

Данная команда позволяет задать максимальное количество безопасных MAC-адресов в системе или на указанной VLAN. При использовании формы **no** команда вернется к настройкам по умолчанию.

port-security limit *VALUE*
no port-security limit

Параметры

VALUE	Укажите максимальное число записей Port Security, которое может быть изучено в системе или в указанной VLAN. Доступен диапазон значений от 1 до 6656. Если указанное значение меньше текущего числа изученных записей, команда будет отклонена.

По умолчанию

По умолчанию в данной опции ограничений нет.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет ограничить количество изученных безопасных MAC-адресов в системе или в VLAN.

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)#
```

58. Команды Power over Ethernet (PoE) Commands (только для ТГК-151-24/4Д-П, ТГК-151-24/4Д-2П и ТГК-151-48/4Д-2П)

58-1 poe pd description

Эта команда используется для настройки описания для PD, подключенного к порту PoE. Используйте **no** для очистки описания.

poe pd description *TEXT*
no poe pd description

Параметры

TEXT	Указывает строку, описывающую PD, подключенный к интерфейсу PoE. Максимальная длина - 32 символа.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для настройки описания PD, подключенного к порту.

Пример

В этом примере показано, как настроить описание PoE PD на порту 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe pd description For VoIP usage
Switch(config-if)#
```

58-2 poe pd legacy-support

Эта команда используется для включения поддержки устаревшего PD. Используйте форму **no** этой команды, чтобы отключить ее.

poe pd legacy-support
no poe pd legacy-support

Параметры

Нет

По умолчанию

По умолчанию эта опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду, чтобы включить поддержку устаревших PD, подключенных к порту. Если поддержка устаревших устройств отключена, система не будет подавать питание на устаревшие PD.

Пример

В этом примере показано, как включить поддержку устаревших технологий для PD, подключенных к порту 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe pd legacy-support
Switch(config-if)#
```

58-3 poe pd priority

Эта команда используется для настройки приоритета для подачи питания на порт. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

poe pd priority {critical | high | low}
no poe pd priority

Параметры

critical	Укажите, что PD, подключенный к порту, имеет наивысший приоритет.
high	Укажите, что PD, подключенный к порту, получает второй высокий приоритет.
low	Укажите, что PD, подключенный к порту, имеет самый низкий приоритет.

По умолчанию

По умолчанию этот параметр установлен как низкий.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Поскольку бюджет мощности ограничен, при добавлении в систему большего количества PD источник питания может оказаться недостаточным для обеспечения питания. Система PoE переходит в критическую секцию питания, когда оставшегося источника питания недостаточно для обслуживания нового добавленного PD. Будет ли подаваться питание на новый добавленный PD, зависит от политики, настроенной командой **poe policy preempt**.

Если параметр вытеснения политики отключен, политика будет обслуживаться в первую очередь. Таким образом, новый PD не будет обслуживаться, если источник питания на исходе. Если параметр вытеснения политики включен, питание, предоставляемое PD с более низким приоритетом, может быть вытеснено, чтобы освободить питание для нового подключенного PD с более высоким приоритетом.

Пример

В этом примере показано, как настроить приоритет порта 1 на первый приоритет.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe pd priority critical
Switch(config-if)#
```

58-4 poe policy preempt

Эта команда используется для разрешения отключения PD, имеющего более низкий приоритет, чтобы в условиях нехватки питания передать питание новому подключенному PD с более высоким приоритетом. Для возврата к настройкам по умолчанию используйте форму **no** этой команды.

poe unit *UNIT-ID* **policy preempt**
no poe unit *UNIT-ID* **policy preempt**

Параметры

UNIT-ID	Указывает идентификатор устройства в конфигурируемом стеке. Этот параметр доступен только при включенном режиме стекирования.

По умолчанию

По умолчанию эта опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Поскольку бюджет питания ограничен, по мере добавления в систему большего количества PD, источник питания может оказаться недостаточным для обеспечения питания. Система PoE переходит в критическую секцию питания, когда оставшегося бюджета питания недостаточно для обслуживания нового добавленного PD.

Команда **poe policy preempt** настраивает, следует ли отключать PD с более низким приоритетом, чтобы передать питание новому подключенному PD с более высоким приоритетом в условиях нехватки питания. Если параметр вытеснения политики отключен, политика будет обслуживаться в первую очередь. Таким образом, новый PD не будет обслуживаться, если бюджет питания исчерпан.

Если параметр вытеснения политики включен, мощность, предоставленная PD с более низким приоритетом, может быть вытеснена, чтобы освободить мощность для нового подключенного PD с более высоким приоритетом.

Пример

В этом примере показано, как настроить вытесняющий режим политики обслуживания питания системы PoE.

```
Switch# configure terminal
Switch(config)# poe unit 1 policy preempt
Switch(config)#
```

58-5 poe power-inline

Эта команда используется для настройки режима управления питанием для портов PoE. Используйте форму **no** этой команды для удаления ассоциации профилей временного диапазона или возврата режима к настройкам по умолчанию.

poe power-inline {auto [max *MAX-WATTAGE*] **[time-range** *PROFILE-NAME*] **| never}**
no poe power-inline [auto {max | time-range}]

Параметры

auto	Указывает, чтобы включить автоматическое обнаружение PD и обеспечить питание PD.
max *MAX-WATTAGE*	(Опционально) Указывается для установки максимальной мощности, которая может быть предоставлена автоопределяемому БП. Если этот параметр не указан, то класс PD автоматически определяет максимальную мощность, которая может быть предоставлена. Диапазон допустимых значений максимальной мощности составляет от 1000 мВт до 30000 мВт.
time-range *PROFILE-NAME*	(Опционально) Указывает имя профиля временного диапазона для разграничения периода активации.
never	Указывает на отключение подачи питания на PD, подключенный к порту.

По умолчанию

По умолчанию этот параметр установлен как **auto**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если порт установлен в auto mode, порт самостоятельно обнаружит PD и обеспечит его питанием. Пользователь может явно указать максимальное значение мощности, которое может быть предоставлено порту. Если максимальное значение мощности не указано, то класс БП автоматически определяет максимальную мощность, которая может быть предоставлена. БП не будет предоставлен, если он запросит мощность, превышающую максимальную.

Используйте эту команду, чтобы также указать временной диапазон для порта. Если порт PoE связан с профилем временного диапазона, он будет активирован только в течение временного интервала, указанного в профиле. То есть, питание на PD не будет подаваться в течение времени, выходящего за рамки указанного временного диапазона.

При выполнении команды **no poe power-inline** режим управления питанием будет возвращен к настройкам по умолчанию.

Для настройки команды указанный профиль временного диапазона не обязательно должен существовать. Если профиль временного диапазона не существует, команда действует так, как будто временной диапазон не указан.

Пример

В этом примере показано, как включить обнаружение PD и автоматически подавать питание на устройство PoE, подключенное к порту 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe power-inline auto
Switch(config-if)#
```

В этом примере показано, как настроить порт PoE 1 на разрешение питания устройств мощностью менее 7000 мВт.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe power-inline auto max 7000
Switch(config-if)#
```

В этом примере показано, как отключить обнаружение PD и не подавать питание на устройство PoE, подключенное к порту 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe power-inline never
Switch(config-if)#
```

В этом примере показано, как объединить профиль временного диапазона под названием "day-time" с портом PoE 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe power-inline auto time-range day-time
Switch(config-if)#
```

58-6 poe usage-threshold

Эта команда используется для настройки порога использования для записи журнала. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

poe unit *UNIT-ID* **usage-threshold** *PERCENTAGE*
no poe unit *UNIT-ID* **usage-threshold**

Параметры

UNIT-ID	Указывает идентификатор устройства в конфигурируемом стеке. Этот параметр доступен только при включенном режиме стекирования.
PERCENTAGE	Указывает порог использования для создания журнала. Диапазон значений от 1 до 99. Единица измерения - процент.

По умолчанию

По умолчанию это значение равно 99.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Когда настроен порог использования, если использование PSE превысит настроенный порог, будет записан журнал EXCEED. Как только процент уменьшится и станет ниже порогового значения, будет записан журнал RECOVER.

Пример

В данном примере показано, как настроить порог использования на 50%.

```
Switch# configure terminal
Switch(config)# poe unit 1 usage-threshold 50
Switch(config)#
```

58-7 snmp-server enable traps poe

Эта команда используется для включения отправки уведомлений PoE. Используйте форму **no** этой команды чтобы отключить отправку уведомлений о питании по Ethernet.

snmp-server enable traps poe [unit *UNIT-ID***]**
no snmp-server enable traps poe [unit *UNIT-ID***]**

Параметры

UNIT-ID	(Опционально) Укажите идентификатор устройства в настраиваемом стеке. Этот параметр доступен только при включенном режиме стекирования.

По умолчанию

По умолчанию эта опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для включения или отключения отправки уведомлений PoE.

Пример

В этом примере показано, как включить отправку уведомлений PoE.

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

58-8 clear poe statistic

Эта команда используется для очистки счетчиков статистики на порту.

clear poe statistic {all | interface *INTERFACE-ID* **[, | -]}**

Параметры

all	Указывает очистку статистики PoE для всех интерфейсов.

interface *INTERFACE-ID*	Указывает идентификатор интерфейса.
,	(Опционально) Указывает серию интерфейсов или отделяет диапазон интерфейсов от предыдущего диапазона. Пробелы до и после запятой не нужны.
-	(Опционально) Указывает диапазон интерфейсов. Без пробелов до и после дефиса.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Для записи статистики на портах имеются счетчики, которые можно показать, введя команду **show poe power-inline statistics command**. Используйте эту команду для очистки всех значений счетчиков на порту.

Пример

В данном примере показано, как очистить статистику на интерфейсе eth1/0/1.

```
Switch# clear poe statistic interface eth1/0/1
Switch#
```

58-9 show poe power-inline

Эта команда используется для отображения статуса PoE для указанного порта PoE или для всех портов PoE на коммутаторе.

show poe power-inline [*INTERFACE-ID* **[, | -]] {status | configuration | statistics | measurement | lldp-classification}**

Параметры

INTERFACE-ID	(Опционально) Укажите интерфейс, который будет отображаться.
,	(Опционально) Указывает серию интерфейсов или отделяет диапазон интерфейсов от предыдущего диапазона. Пробелы до и после запятой не нужны.
-	(Опционально) Указывает диапазон интерфейсов. Без пробелов до и после дефиса.
status	Указывает для отображения состояния порта PoE.
configuration	Указывает на отображение информации о конфигурации порта.
statistics	Указывает на отображение счетчиков ошибок порта.

measurement	Указывает для отображения напряжения, тока, потребляемой мощности и температуры порта.
lldp-classification	Указывает на отображение классификации уровня канала данных с использованием информации о мощности через MDI TLV.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Эта команда используется для отображения статуса PoE портов, состояния конфигурации линии электропитания, счетчиков статистики, результатов измерений и информации о классификации уровня канала передачи данных. Если ID интерфейса не указан в этой команде, то будут отображены все интерфейсы PoE. Отображаются только интерфейсы с поддержкой PoE.

Пример

В этом примере показано, как отобразить состояние питания PoE в линии.

```
Switch#show poe power-inline status

Interface   State      Class   Max(W) Used(W) Description
------------------------------------------------------------------------------
eth1/0/1    delivering class-1 7.0    3.4     For VoIP usage
eth1/0/2    searching  n/a     0.0    0.0
eth1/0/3    searching  n/a     0.0    0.0
eth1/0/4    searching  n/a     0.0    0.0
eth1/0/5    searching  n/a     0.0    0.0
eth1/0/6    searching  n/a     0.0    0.0
eth1/0/7    searching  n/a     0.0    0.0
eth1/0/8    searching  n/a     0.0    0.0
eth1/0/9    searching  n/a     0.0    0.0
eth1/0/10   searching  n/a     0.0    0.0
eth1/0/11   searching  n/a     0.0    0.0
eth1/0/12   searching  n/a     0.0    0.0
eth1/0/13   searching  n/a     0.0    0.0
eth1/0/14   searching  n/a     0.0    0.0
eth1/0/15   searching  n/a     0.0    0.0
eth1/0/16   searching  n/a     0.0    0.0
eth1/0/17   searching  n/a     0.0    0.0
eth1/0/18   searching  n/a     0.0    0.0
eth1/0/19   searching  n/a     0.0    0.0
eth1/0/20   searching  n/a     0.0    0.0
eth1/0/21   searching  n/a     0.0    0.0
eth1/0/22   searching  n/a     0.0    0.0
eth1/0/23   searching  n/a     0.0    0.0
eth1/0/24   searching  n/a     0.0    0.0

Faulty code
[1] MPS (Maintain Power Signature) Absent
[2] PD short
[3] Overload
[4] Power Denied
[5] Thermal Shutdown
[6] Startup Failure
[7] Classification Failure

Switch#
```

Отображаемые параметры

Interface	Идентификатор интерфейса PoE.
State	Состояние порта может быть одним из следующих: **Disabled**: Функция PSE отключена.

	Searching: Удаленный PD не подключен. **Requesting** (запрос): Удаленный БП подключен, но PSE еще не подает питание. **Delivering**: Удаленный БП получает питание от системы PoE. **Faulty**[X]: Обнаружение устройства или питаемое устройство находится в неисправном состоянии. X -это номер кода ошибки. [1] - MPS (Maintain Power Signature) Отсутствует. [2] - Короткое замыкание БП. [3] - Перегрузка. [4] - Отказ в питании. [5] - Тепловое отключение. [6] - Сбой запуска. [7] - Сбой классификации (IEEE 802.3at).
Class	Классификация IEEE: N/A или значение из класса IEEE от 0 до 4.
Max(W)	Максимальное количество мощности, которое может быть выделено питаемому устройству в ваттах.
Used(W)	Количество энергии, выделяемой в настоящее время портам PoE, в ваттах.
Description	Сконфигурированное описание подключенного PD.

В этом примере показано, как отобразить конфигурацию PoE power inline.

```
Switch#show poe power-inline configuration

Interface Admin   Priority  Legacy-Support  Time-Range
-----------------------------------------------------------------
eth1/0/1  auto(M) critical  enabled
eth1/0/2  auto    low       disabled
eth1/0/3  auto    low       disabled
eth1/0/4  auto    low       disabled
eth1/0/5  auto    low       disabled
eth1/0/6  auto    low       disabled
eth1/0/7  auto    low       disabled
eth1/0/8  auto    low       disabled
eth1/0/9  auto    low       disabled
eth1/0/10 auto    low       disabled
eth1/0/11 auto    low       disabled
eth1/0/12 auto    low       disabled
eth1/0/13 auto    low       disabled
eth1/0/14 auto    low       disabled
eth1/0/15 auto    low       disabled
eth1/0/16 auto    low       disabled
eth1/0/17 auto    low       disabled
eth1/0/18 auto    low       disabled
eth1/0/19 auto    low       disabled
eth1/0/20 auto    low       disabled
eth1/0/21 auto    low       disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Отображаемые параметры

Interface	Идентификатор интерфейса PoE.
Admin	Настраиваемый пользователем режим может быть одним из следующих: **Auto** (Авто): устройство с питанием будет автоматически обнаружено, а максимальная мощность будет основана на результатах обнаружения. **Auto(M)**: Питаемое устройство будет автоматически обнаружено, а максимальная мощность будет равна значению, настроенному пользователем. Никогда: Питаемое устройство не будет обнаружено, и питание на порт не подается.
Priority	Приоритет, используемый для определения очередности обслуживания при ограничении мощности в пределах энергоблока.
Legacy-Support	**Enabled** (Включено): Устаревший БП может быть обнаружен. **Disabled**: Устаревший БП не может быть обнаружен.

Time-Range	Имя профиля временного диапазона, который устанавливает временные рамки активации для порта.

В этом примере показано, как отобразить статистику PoE power inline.

```
Switch#show poe power-inline statistics

Interface  MPS Absent  Overload  Short  Power Denied  Invalid Signature
---------  ----------  --------  -----  ------------  -----------------
eth1/0/1       2           5       0        10              7
eth1/0/2       0           0       0        0               9
eth1/0/3       0           0       0        0               9
eth1/0/4       0           0       0        0               10
eth1/0/5       0           0       0        0               157
eth1/0/6       0           0       0        0               157
eth1/0/7       0           0       0        0               156
eth1/0/8       0           0       0        0               158
eth1/0/9       0           0       0        0               166
eth1/0/10      0           0       0        0               165
eth1/0/11      0           0       0        0               165
eth1/0/12      0           0       0        0               166
eth1/0/13      0           0       0        0               143
eth1/0/14      0           0       0        0               143
eth1/0/15      0           0       0        0               143
eth1/0/16      0           0       0        0               144
eth1/0/17      0           0       0        0               166
eth1/0/18      0           0       0        0               166
eth1/0/19      0           0       0        0               166
eth1/0/20      0           0       0        0               161
eth1/0/21      0           0       0        0               163
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Отображаемые параметры

MPS Absent	Увеличивается, если PSE перестает подавать питание на PI из-за того, что PSE не может контролировать действующие MPS PD на PI.
Overload	Если PD потребляет слишком много энергии, превышая максимальную выходную мощность, которую может обеспечить порт, счетчик перегрузки увеличивается.
Short	Если внутренняя цепь PD по какой-то причине закорочена, этот счетчик увеличивается.
Power Denied	Если программная система PoE решает запретить подачу питания на подключенный PD, этот счетчик увеличивается.
Invalid Signature	Увеличивается, если PSE обнаруживает PD, у которого недействительная подпись PD.

В этом примере показано, как отобразить измерение мощности PoE в линии.

```
Switch#show poe power-inline measurement

Interface  Voltage(V)  Current(mA)  Temperature(C)  Power(W)
---------  ----------  -----------  --------------  ---------
eth1/0/1     54.2         109           35            5.9
eth1/0/2     n/a          n/a           n/a           n/a
eth1/0/3     n/a          n/a           n/a           n/a
eth1/0/4     n/a          n/a           n/a           n/a
eth1/0/5     n/a          n/a           n/a           n/a
eth1/0/6     n/a          n/a           n/a           n/a
eth1/0/7     n/a          n/a           n/a           n/a
eth1/0/8     n/a          n/a           n/a           n/a
eth1/0/9     n/a          n/a           n/a           n/a
eth1/0/10    n/a          n/a           n/a           n/a
eth1/0/11    n/a          n/a           n/a           n/a
eth1/0/12    n/a          n/a           n/a           n/a
eth1/0/13    n/a          n/a           n/a           n/a
eth1/0/14    n/a          n/a           n/a           n/a
eth1/0/15    n/a          n/a           n/a           n/a
eth1/0/16    n/a          n/a           n/a           n/a
eth1/0/17    n/a          n/a           n/a           n/a
eth1/0/18    n/a          n/a           n/a           n/a
eth1/0/19    n/a          n/a           n/a           n/a
eth1/0/20    n/a          n/a           n/a           n/a
eth1/0/21    n/a          n/a           n/a           n/a
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

В этом примере показано, как отобразить классификацию PoE power inline LLDP.

```
Switch# show poe power-inline lldp-classification

Interface eth1/0/1
PSE TX information:

Power type; type 2 PSE
Power source: primary power source
Power priority: low
PD requested power value: 25.0W
PSE allocated power value: 25.0W

Information from PD:

Power type: type 2 PD
Power source: PSE
Power priority: unknown
PD requested power value: 25.0W
PSE allocated power value: 25.0W

Interface eth1/0/2
PSE TX information:

Power type; type 2 PSE
Power source: primary power source
Power priority: high
PD requested power value: 0.0W
PSE allocated power value: 0.0W

Information from PD:

none

Interface eth1/0/3
PSE TX information:

Power type; type 2 PSE
Power source: primary power source
Power priority: low
PD requested power value: 20.0W
PSE allocated power value: 20.0W

Information from PD:

Power type: type 2 PD
Power source: PSE
Power priority: unknown
PD requested power value: 20.0W
PSE allocated power value: 20.0W

Switch#
```

Отображаемые параметры

Interface	Идентификатор интерфейса PoE.
Power type	Поле типа питания, которое находится в Power via MDI TLV из PSE или PD LLDP-пакета.
Power source	Поле источника питания, которое находится в Power via MDI TLV из PSE или PD LLDP-пакета.
Power priority	Поле приоритета мощности, которое находится в Power via MDI TLV из PSE или PD LLDP-пакета.
PD requested power value	Поле значения мощности, запрашиваемой PD, которое находится в TLV Power via MDI из PSE или PD LLDP-пакета.
PSE allocated power value	Поле значения мощности, выделенной PSE, которое находится в Power via MDI TLV из PSE или PD LLDP-пакета.

58-10 show poe power module

Эта команда используется для отображения настроек и фактических значений силовых модулей.

show poe power module [unit *UNIT-ID***] [detail]**

Параметры

UNIT-ID	(Опционально) Указывает идентификатор устройства в стеке, который будет отображаться. Этот параметр доступен только при включенном режиме стекирования.
detail	(Опционально) Указывает на отображение более подробной информации о параметрах микросхемы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Эта команда отображает подробную информацию о питании и параметры чипа PoE для модулей PoE.

Пример

В этом примере показано, как отобразить информацию о мощности системы питания PoE.

```
Switch#show poe power module

Unit Delivered(W)  Power Budget(W)  Usage-Threshold(%)   Preempt   Trap State
------------------------------------------------------------------------------
1      0             370                99              Enabled    Disabled

Switch#
```

Отображаемые параметры

Unit	Идентификатор устройства стекирования.
Delivered	Фактическая мощность, подаваемая на PD, в ваттах.
Power budget	Общая мощность, которую может обеспечить устройство, в ваттах.
Usage-Threshold	Порог использования для записи журнала.
Preempt	**Enabled**: Режим управления питанием - вытеснение политики, PD с высоким приоритетом может вытеснять питание PD с более низким приоритетом. **Disabled**: Режим управления питанием - "первый обслуживается первым".
Trap State	**Enabled** (Включено): Ловушка отправляется, когда порог использования PoE превышает указанное значение. **Disabled** (Отключено): Ловушка не отправляется, когда порог использования PoE превышает указанное значение.

В данном примере показано, как отобразить подробные параметры PoE для устройства 1.

```
Switch#show poe power module unit 1 detail

Unit Delivered(W)  Power Budget(W)  Usage-Threshold(%)   Preempt   Trap State
------------------------------------------------------------------------------
1      0             370                99              Enabled    Disabled

PoE system parameters:
Unit   Max Ports   Device ID    SW Version
----   ---------   ---------    ----------
1      24          E111         17

Switch#
```

Отображаемые параметры

Max ports	Максимальный номер порта подсистемы PoE.
Device ID	Аппаратная версия чипа PoE.
S/W version	Версия микропрограммы чипа PoE.

58-11 poe pd alive

Эта команда используется для включения функции проверки жизни PD для PD, подключенного к порту PoE. Для отключения функции используйте форму **no** этой команды.

poe pd alive [{ip *IP-ADDRESS* **| interval** *INTERVAL-TIME* **| retry** *RETRY-COUNT* **| waiting-time** *WAITING-TIME* **| action {reset | notify | both}}]**
no poe pd alive [{ip | interval | retry | waiting-time | action}]

Параметры

ip	(Опционально) Указывает IPv4-адрес целевого PD для системы, выполняющей действие ping.
interval	(Опционально) Указывает интервал, в течение которого система будет отправлять запросы ping для обнаружения целевого PD. Допустимый диапазон - от 10 до 300 секунд.
retry	(Опционально) Указывает количество повторных попыток запросов ping, когда PD не получил ответа. Допустимый диапазон - от 0 до 5.
waiting-time	(Опционально) Указывает время ожидания восстановления PD после перезагрузки. Диапазон допустимых значений составляет от 30 до 300 секунд.
action	(Опционально) Указывает действие системы, когда PD не отвечает на запрос ping. **reset** - Указывает отключение и последующее включение состояния порта PoE. **notify** - Указывает отправку журналов и ловушек для уведомления администратора. **both** - Указывает сначала отправить журнал и ловушку, а затем сбросить состояние порта PoE.

По умолчанию

По умолчанию эта функция отключена.
По умолчанию IP-адрес целевого PD не задан.
По умолчанию интервал между запросами ping для системы составляет 30 секунд.
Количество повторных попыток для запросов ping по умолчанию - 2 раза.
Время ожидания по умолчанию для восстановления PD после перезагрузки составляет 90 секунд.
Действие по умолчанию, когда PD не отвечает на запрос ping, - **both**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта функция действует только на портах с поддержкой PoE и подачей питания.

Функция проверки работоспособности PD обеспечивает решение для PD-устройства, которое перестает работать или не отвечает на запросы через механизм ping.

Используйте эту команду без параметров, чтобы включить или отключить функцию проверки PD.
По умолчанию IP-адрес целевого PD отсутствует, чтобы система могла выполнить действие ping. IP-адрес целевого PD должен быть настроен с помощью команды **poe pd alive ip** перед выполнением проверки работоспособности PD.

Системе необходимо периодически отслеживать определенный PD с помощью функции ping. При отсутствии ответа система предпринимает одно из действий, настроенных командой **poe pd alive action**. Интервал между повторными попытками может быть настроен командой **poe pd alive interval**.

Система реализует механизм повторных попыток для проверки состояния PD. Система сбросит питание порта PoE после повторной попытки с помощью Ping при отсутствии ответа от PD. Количество повторных попыток может быть настроено командой **poe pd alive retry**.

Если действие **reset** или **both**, системе необходимо подождать, пока PD восстановится после перезагрузки, а затем снова выполнить функцию Ping. Время ожидания восстановления PD после перезагрузки можно настроить с помощью команды **poe pd alive waiting-time**.

Если функция диапазона времени PoE настроена на порту, на котором также включена функция проверки жизни PD, функция диапазона времени имеет более высокий приоритет, и функция проверки жизни PD не будет работать, когда функция диапазона времени PoE все еще активна.

ПРИМЕЧАНИЕ: Если PD не поддерживает ICMP, эта функция не сможет нормально работать.

ПРИМЕЧАНИЕ: Необходимо правильно настроить параметры IP, чтобы до PD можно было добраться через Ping, иначе эта функция не сможет работать должным образом.

ПРИМЕЧАНИЕ: Действие сброса может работать только на PD, подключенном напрямую. Если PD подключен не напрямую, действие сброса может не сработать должным образом.

ПРИМЕЧАНИЕ: Если PD, подключенный напрямую, также является PSE, все PD следующего уровня, подключенные к этому PSE, будут зацикливаться при каждом действии функции проверки жизни PD при reset или both действиях.

Пример

В этом примере показано, как включить функцию проверки жизни PoE PD на портах 1 - 2.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/1-2
Switch(config-if-range)#poe pd alive
Switch(config-if-range)#
```

В этом примере показано, как настроить IP-адрес целевого PD.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive ip 192.168.1.150
Switch(config-if)#
```

В этом примере показано, как настроить интервал между запросами ping.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive interval 60
Switch(config-if)#
```

В этом примере показано, как настроить количество повторных попыток для запросов ping.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive retry 4
Switch(config-if)#
```

В этом примере показано, как настроить время ожидания перезагрузки PD.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive waiting-time 120
Switch(config-if)#
```

В этом примере показано, как настроить действие на сброс, когда PD не отвечает.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive action reset
Switch(config-if)#
```

58-12 show poe pd alive

Эта команда используется для отображения настроек проверки жизни PD.

show poe pd alive [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	Указывает идентификатор интерфейса для отображения.
,	(Опционально) Указывает серию интерфейсов или отделяет диапазон интерфейсов от предыдущего диапазона. Пробел до и после запятой не ставится.
-	(Опционально) Указывает диапазон интерфейсов. Пробел до и после дефиса не ставится.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду для отображения настроек проверки жизни PD на указанных портах. Если дополнительный параметр не указан, будет отображена информация обо всех портах PoE.

Пример

В этом примере показано, как отобразить настройки проверки PD alive check на портах 1 - 2.

```
Switch#show poe pd alive interface eth1/0/1-2

Port ID: eth1/0/1
-------------------------------------------
    PD Alive State                : Disabled
    PD IP Address                 : 0.0.0.0
    Poll Interval                 : 30
    Retry Count                   : 2
    Waiting Time                  : 90
    Action                        : both
Port ID: eth1/0/2
-------------------------------------------
    PD Alive State                : Disabled
    PD IP Address                 : 192.168.1.150
    Poll Interval                 : 30
    Retry Count                   : 4
    Waiting Time                  : 120
    Action                        : reset

Switch#
```

59. Команды энергосбережения

59-1 dim led

Данная команда используется для отключения индикаторов портов с целью энергосбережения. Используйте форму **no**, чтобы не отключать индикаторы портов с целью энергосбережения.

dim led
no dim led

Параметры

Нет

По умолчанию

По умолчанию эта опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы отключить индикаторы портов с целью энергосбережения. Используйте форму no, чтобы не отключать индикаторы портов с целью энергосбережения. 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)#
```

59-2 power-saving

Данная команда используется для включения отдельных функций энергосбережения. Используйте форму **no**, чтобы отключить данные функции.

power-saving {link-detection | port-shutdown | dim-led | hibernation}
no power-saving {link-detection | length-detection | port-shutdown | dim-led | hibernation}

Параметры

link-detection	Укажите, чтобы включать функцию энергосбережения в

	зависимости от статуса соединения.
port-shutdown	Укажите, чтобы включать функцию энергосбережения по расписанию отключения индикаторов.
dim-led	Укажите, чтобы включать функцию энергосбережения по расписанию отключения порта.
hibernation	Укажите, чтобы включать функцию энергосбережения по расписанию режима сна системы. Данная функция не поддерживается коммутаторами, объединенными в физический стек.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

С помощью этой команды пользователь может включить или отключить обнаружение соединения, затемнение светодиодов, выключение порта и спящий режим.

Если функция обнаружения соединения включена, устройство может экономить энергию на неактивных портах.

Если включено затемнение светодиодов, устройство будет выключать все светодиоды порта в указанном диапазоне времени для экономии энергии.

Если включено отключение порта, устройство отключит все порты в указанном диапазоне времени для экономии энергии.

Если включен режим гибернации, устройство перейдет в режим гибернации в указанном диапазоне времени для экономии энергии. Этот параметр можно использовать только в том случае, если режим стекирования отключен.

Пример

В данном примере показано, как отключить порты и перейти в режим сна для энергосбережения.

```
Switch# configure terminal
Switch(config)# power-saving port-shutdown
Switch(config)# power-saving hibernation
Switch(config)#
```

59-3 power-saving eee

Данная команда используется для включения функции Energy-Efficient Ethernet (EEE) на определенном порту/портах. Используйте форму **no**, чтобы отключить функцию EEE.

power-saving eee
no power-saving eee

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для включения или отключения функции Energy-Efficient Ethernet (EEE) на определенном порту/портах. В режиме Power-Saving EEE энергосбережение зависит от использования фактической пропускной способности и будет обеспечено при установленном соединении во время низкого использования трафика пакетов. Если передаваемые данные отсутствуют, на физическом интерфейсе будет включен режим Low Power Idle (LPI).

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)#
```

59-4 power-saving dim-led time-range

Данная команда используется для настройки профиля временного диапазона для расписания отключения индикаторов (Dim LED). Используйте форму **no**, чтобы удалить профиль указанного диапазона времени.

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. Максимально допустимое количество символов – 32.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы добавить/удалить профиль временного диапазона для расписания отключения индикаторов (Dim LED). Если расписание настроено, все индикаторы порта будут отключены.

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)#
```

59-5 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. Максимально допустимое количество символов – 32.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 не действуют сетевые

функции. 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)#
```

59-6 power-saving shutdown time-range

Данная команда используется для настройки профиля временного диапазона для расписания отключения порта (Port Shutdown). Используйте форму **no**, чтобы удалить профиль указанного диапазона времени.

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. Максимально допустимое количество символов – 32.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы добавить/удалить профиль временного диапазона для расписания отключения порта (Port Shutdown). Если расписание настроено, указанный порт будет отключен.

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)#
```

59-7 show power-saving

Данная команда используется для отображения информации о настройках энергосбережения.

show power-saving [link-detection] [length-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 настройки энергосбережения за счет отключения индикаторов.
port-shutdown	(Опционально) Укажите, чтобы отобразить настройки энергосбережения за счет отключения порта.
hibernation	(Опционально) Укажите, чтобы отобразить настройки энергосбережения для режима сна.
eee	(Опционально) Укажите, чтобы отобразить настройки энергосбережения для функции EEE.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Если ни один из опциональных параметров не указан, будет отображена информация о всех настройках энергосбережения.

Пример

В данном примере показано, как отобразить информацию о всех настройках энергосбережения.

```
Switch#show power-saving
Function Version: 3.00

Link Detection 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
  eth1/0/1

Switch#
```

60. Команды Protocol Independent

60-1 ip route

Эта команда используется для создания записи статического маршрута. Используйте форму **no** этой команды, чтобы удалить запись статического маршрута.

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 (Next Hop), который будет использоваться для достижения сети назначения.
primary	(Опционально) Укажите маршрут как основной маршрут к назначению.
backup	(Опционально) Укажите маршрут как резервный маршрут к назначению.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Доступны плавающие маршруты. Это означает, что можно создать два маршрута с одни адресом сети назначения, но с разными следующими узлами (Next Hop). Если ни один из параметров (**primary** или **backup**) не указан, роль статического маршрута (основной/резервный) будет назначена автоматически. Основной маршрут (Primary) является самым приоритетным и всегда используется для продвижения, если находится в активном режиме. Если основной маршрут неактивен, используется резервный маршрут (Backup).

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)#
```

60-2 ipv6 route

Данная команда используется для создания записи статического маршрута IPv6. Используйте форму **no**, чтобы удалить запись статического маршрута IPv6.

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) Укажите маршрут как основной маршрут к назначению.
backup	(Опционально) Укажите маршрут как резервный маршрут к назначению.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Доступны плавающие маршруты. Это означает, что можно создать два маршрута с одни адресом сети назначения, но с разными следующими узлами (Next Hop). Если ни один из параметров (**primary** или **backup**) не указан, роль статического маршрута (основной/резервный) будет назначена автоматически. Основной маршрут (Primary) является самым приоритетным и всегда используется для продвижения, если находится в активном режиме. Если основной маршрут неактивен, используется резервный маршрут (Backup).

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 vlan 1 fe80::0000:00ff:1111:2233
Switch(config)#
```

60-3 show ip route

Данная команда используется для отображения записи в таблице 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) Указывает отображение маршрута с прямым подключением.
static	(Опционально) Указывает отображение статического маршрута.
hardware	(Опционально) Указывает отображение маршрутов, которые были записаны в микросхему.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду для отображения лучших маршрутов, которые в настоящее время работают.

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#
```

60-4 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется 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#
```

60-5 show ipv6 route

Эта команда используется для отображения записи в таблице маршрутизации.

show ipv6 route [[*IPV6-ADDRESS* **|** *NETWORK-PREFIX/PREFIX-LENGTH* **[longer-prefixes] |** *INTERFACE-ID* **| connected | static] [database] | hardware]**

Параметры

IPV6-ADDRESS	(Опционально) Укажите IPv6-адрес, чтобы найти самый длинный префикс соответствующего IPv6-маршрута.
NETWORK-PREFIX	(Опционально) Укажите сетевой адрес, информацию о маршрутизации которого необходимо отобразить.
PREFIX-LENGTH	(Опционально) Укажите длину префикса для указанной сети.
longer-prefixes	(Опционально) Указывает отображение маршрута и всех более конкретных маршрутов.
INTERFACE-ID	(Опционально) Укажите интерфейс, который будет использоваться при отображении.
connected	(Опционально) Указывает отображение маршрута с прямым подключением.
static	(Опционально) Указывает отображение статического маршрута.
database	(Опционально) Указывает на отображение всех связанных записей в базе данных маршрутизации, а не только наилучшего маршрута.
hardware	(Опционально) Указывает отображение маршрутов, которые были записаны в микросхему.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду для отображения лучших маршрутов, которые в настоящее время работают.

Пример

В данном примере показано, как отобразить записи маршрутизации для IPv6.

```
Switch# show ipv6 route

IPv6 Routing Table
Code: C - connected, S - static

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#
```

В данном примере показано отображение записей статической маршрутизации для IPv6.

```
Switch# show ipv6 route static

IPv6 Routing Table
Code: C - connected, S - static

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: 2 entries, 2 routes

Switch#
```

60-6 show ipv6 route summary

Данная команда используется для отображения текущего состояния таблицы маршрутизации IPv6.

show ipv6 route summary

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Если система обслуживания обеспечивает продвижение IPv6-трафика, необходимо проверять таблицу переадресации/маршрутизации для выявления пути трафика, который будет использоваться в сети.

Пример

В данном примере показано, как отобразить текущее состояние таблицы маршрутизации IPv6.

```
Switch# show ipv6 route summary

Route Source    Networks
Connected       2
Static          1
Total           3

Switch#
```

61. Команды качества обслуживания (QOS)

61-1 class

Данная команда используется для указания имени карты класса (Class-map) для привязки к политике трафика с дальнейшем переходом в режим Policy-map Configuration Mode. Используйте форму **no**, чтобы удалить описание политики указанного класса.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

После ввода данной команды будет выполнен вход в режим Policy-map Configuration Mode. Весь траффик, который не соответствует текущему настроенному классу, будет классифицирован как класс по умолчанию (Class-Default). Если указанное имя карты класса не существует, никакой траффик 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 при использовании Single Rate Policer.

```
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)# police 1000000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)#
```

61-2 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. Используйте форму **no**, чтобы удалить существующую карту класса на коммутаторе.

class-map [match-all | match-any] *NAME*
no class-map *NAME*

Параметры

NAME	Укажите имя карты класса. Максимально допустимое количество символов – 32.
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**.
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**.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 настроено 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. Настроенное 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 настроенную 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)#
```

61-3 match

Данная команда используется для настройки критериев соответствия для карты класса. Используйте форму **no**, чтобы удалить критерии соответствия.

match {access-group name *ACCESS-LIST-NAME* **| cos [inner]** *COS-LIST* **| [ip] dscp** *DSCP-LIST* **|[ip] precedence** *IP-PRECEDENCE-LIST* **| protocol** *PROTOCOL-NAME* **| vlan [inner]** *VLAN-LIST***}**

no match {access-group name *ACCESS-LIST-NAME* **| cos [inner]** *COS-LIST* **| [ip] dscp** *DSCP-LIST* **| [ip] precedence** *IP PRECEDENCE-LIST* **| protocol** *PROTOCOL-NAME* **| vlan [inner]** *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 [inner] *COS-LIST*	Укажите значение(я) определенного IEEE 802.1Q в качестве критерия соответствия. Доступный 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. Доступный 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, проверка критерий настраивается для пакетов IPv4 и IPv6.
[ip] precedence *IP-PRECEDENCE-LIST*	Укажите значения приоритета IP в качестве критерия соответствия. Доступный 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 [inner] *VLAN-LIST*	Укажите номер(а) или диапазон номеров идентификации VLAN в качестве критерия соответствия. Доступный 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

Уровень команды по умолчанию

Уровень 12

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 настроенной карты класса – class-home-user. Имя настроенного 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 данном примере показано, как настроить карту класса и значения CoS, которые будут использованы в качестве критериев соответствия для данного класса. Имя настроенной карты класса – cos. Настроенные 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)#
```

В данном примере показано, как настроить классы для классификации трафика на основе значений CoS. Имена настроенных классов: voice и video-n-data. Обработка QoS предназначена для соответствующих пакетов в карте политики «cos-based-treatment». Для обработки QoS класса «voice» используется Single Rate Policer, для класса «video-n-data» – Two Rate Policer. Настроенная политика обслуживания привязана к интерфейсу Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# class-map voice
Switch(config-cmap)# match cos 7
Switch(config-cmap)# exit
Switch(config)# class-map video-n-data
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
Switch(config)# policy-map cos-based-treatment
Switch(config-pmap)# class voice
Switch(config-pmap-c)# police 8000 1000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video-n-data
Switch(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 exceed-action set-dscp-
transmit 2 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# service-policy input cos-based-treatment
Switch(config-if)#
```

61-4 mls qos aggregate-policer

Данная команда используется для настройки Aggregate Policer, который будет использован в картах политики. Используйте форму no, чтобы удалить Aggregate Policer. Команда **mls qos aggregate-policer** применяется для использования Single Rate Policing, а команда **mls qos aggregate-policer cir** для использования Two Rate Policing.

mls qos aggregate-policer *NAME KBPS* **[***BURST-NORMAL* **[***BURST-MAX***]] [conform-action** *ACTION***] exceed-action** *ACTION* **[violate-action** *ACTION***] [color-aware]**

mls qos aggregate-policer *NAME* **cir** *CIR* **[bc** *CONFORM-BURST***] pir** *PIR* **[be** *PEAK-BURST***][conform-action** *ACTION***] [exceed-action** *ACTION* **[violate-action** *ACTION***]] [color-aware]**

no mls qos aggregate-policer *NAME*

Параметры

NAME	Укажите имя правила Aggregate Policing. Максимально допустимое количество символов – 32. Символы, используемые в данном параметре, чувствительны к регистру. Имена Aggregate Policer не должны совпадать и начинаться с цифры. Первым символом в имени обязательно должна быть буква.
KBPS	Укажите среднюю скорость в Кбит/с.

BURST-NORMAL	(Опционально) Укажите нормальный размер всплеска (Burst). Единица измерения – Кбайт.
BURST-MAX	(Опционально) Укажите максимальный размер всплеска (Burst). Единица измерения – Кбайт.
CIR	Укажите гарантированную полосу пропускания (Committed Information Rate) в Кбит/с. Данный параметр является первым в алгоритме «корзина маркеров» (Token Bucket) для Two-rate Metering.
PIR	Укажите пиковую скорость передачи (Peak Information Rate) в Кбит/с. Данный параметр является вторым в алгоритме «корзина маркеров» (Token Bucket) для Two-rate Metering.
PEAK-BURST	(Опционально) Укажите размер всплеска (Burst) для первого параметра алгоритма «корзина маркеров» (Token Bucket). Единица измерения – Кбайт.
conform-action	(Опционально) Укажите, чтобы действие было выполнено к Green Color Packets (пакетам, «окрашенным» в зелёный цвет). Если не указано, будет выполнено действие по умолчанию **transmit** (передача пакетов).
exceed-action	Укажите, чтобы действие было выполнено к пакетам, превышающим разрешенную скорость. Если при использовании Two Rate Policer данный параметр не указан, будет выполнено действие по умолчанию **drop** (отбрасывание).
violate-action	(Опционально) Укажите, чтобы при использовании Single Rate Policing действие было выполнено к пакетам, нормальный и максимальный размеры всплеска которых не соответствуют заданным параметрам. Укажите, чтобы действие было выполнено к пакетам, не соответствующим обоим параметрам CIR и PIR. Если при использовании Single Rate Policer данный параметр не указан, будет создан Single Rate Two Color Policer. Если при использовании Two Rate Policer данный параметр не указан, будет выполнено действие по умолчанию **drop** (отбрасывание).
ACTION	Укажите, чтобы действие было выполнено к пакетам. Ниже указаны ключевые слова: **drop** – отбрасывание пакетов. **set-dscp-transmit** *VALUE* – укажите значение IP DSCP-метки и передачупакетов с новой IP DSCP-меткой. **set-1p-transmit** – укажите значение 802.1p и передачу пакетов с новым значением. **transmit** – передача пакетов без изменений.
color-aware	(Опционально) Укажите данный параметр для Single Rate Three Color Policer или Two Rate Three Color Policer. Если данный параметр не указан, Policer работает в режиме Color Blind. Если данный параметр указан, Policer работает в режиме Color Aware.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Aggregate Policer может быть общим для разных классов в карте политики. Для разных карт политики настройка общего Aggregate Policer невозможна.

Пример

В данном примере показано, как настроить Aggregate Policer с использованием Single Rate Two Color Policer. Настроенное имя Aggregate Policer – agg-policer5. Данный Aggregate Policer применен в качестве политики обслуживания для классов трафика 1 и 2 (class1, class2) в карте политики «policy 2».

```
Switch# configure terminal
Switch(config)# mls qos aggregate-policer agg-policer5 10 1000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer5
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police aggregate agg_policer5
Switch(config-pmap-c)#
```

61-5 mls qos cos

Данная команда используется для настройки значения CoS по умолчанию для порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

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.

CoS по умолчанию пакетов, поступающих на порт 802.1Q VLAN tunnel, имеет два значения: внутренний CoS, назначенный пакету, и CoS в теге VLAN tunnel передаваемого пакета.

Пример

В данном примере показано, как настроить значение CoS по умолчанию на Ethernet-порту 1/0/1. Настроенное значение – 3.

```
Switch# configure terminal
Switch(config)# interface  ethernet 1/0/1
Switch(config-if)# mls qos cos 3
Switch(config-if)#
```

61-6 mls qos dscp-mutation

Данная команда используется для привязки карты изменения входящего DSCP (DSCP Mutation) к интерфейсу. Используйте форму **no**, чтобы удалить привязку карты DSCP Mutation к интерфейсу.

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. Максимально допустимое количество символов – 32.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 порту 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 ethernet 1/0/1
Switch(config-if)# mls qos dscp-mutation mutemap1
Switch(config-if)#
```

61-7 mls qos map cos-color

Данная команда используется для настройки цветовой привязки CoS пакета. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

mls qos map cos-color *COS-LIST* **to {green | yellow | red}**
no mls qos map cos-color

Параметры

COS-LIST	Укажите список значений CoS для привязки к цвету. Доступный диапазон значений: от 0 до 7. Несколько значений CoS могут быть отделены запятой или списком диапазонов.
green	Укажите для привязки к зеленому цвету.
yellow	Укажите для привязки к желтому цвету.
red	Укажите для привязки к красному цвету.

По умолчанию

По умолчанию все значения CoS привязаны к зеленому цвету.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Пакеты, поступающие на входной порт, могут быть «окрашены» на основе цветовой привязки DSCP (если порт является доверенным портом DSCP) или на основе цветовой привязки CoS (если порт является доверенным портом CoS).

Используйте данную команду в режиме Interface Configuration Mode, чтобы настроить цветовую привязку CoS. Если входной порт является доверенным портом CoS, полученный пакет будет инициализирован с цветом на основе настроенной привязки.

Пример

В данном примере показано, как настроить цветовую привязку CoS пакетов, поступающих на интерфейс Ethernet 1/0/1. Пакеты со значением CoS от 1 до 7 привязаны к красному цвету, а пакеты со значением 0 – к зеленому.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# mls qos map cos-color 1-7 to red
Switch(config-if)#
```

61-8 mls qos map dscp-color

Данная команда используется для настройки цветовой привязки DSCP пакета. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

mls qos map dscp-color *DSCP-LIST* **to {green | yellow | red}**
no mls qos map dscp-color *DSCP-LIST*

Параметры

DSCP-LIST	Укажите список DSCP-меток для привязки к цвету. Доступный диапазон значений: от 0 до 63. Несколько значений DSCP могут быть отделены запятой или списком диапазонов.
green	Укажите для привязки к зеленому цвету.
yellow	Укажите для привязки к желтому цвету.
red	Укажите для привязки к красному цвету.

По умолчанию

По умолчанию привязка не настроена. Все значения DSCP привязаны к зеленому цвету.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки цветовой привязки DSCP пакета.

Пример

В данном примере показано, как привязать пакеты с DSCP-меткой от 61 до 63 к желтому цвету на интерфейсе Ethernet 1/0/1. Другие IP-пакеты будут инициализированы с зеленым цветом.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# mls qos map dscp-color 61-63 to yellow
Switch(config-if)#
```

61-9 mls qos map dscp-cos

Данная команда используется для привязки DSCP-меток к CoS. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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. Доступный диапазон значений: от 0 до 63. Несколько DSCP могут быть отделены запятой (,) или дефисом (-). Пробелы до и после дефиса 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

Уровень команды по умолчанию

Уровень 12

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 ethernet 1/0/6
Switch(config-if)# mls qos map dscp-cos 12,16,18 to 1
Switch(config-if)#
```

61-10 mls qos map dscp-mutation

Данная команда используется для настройки карты DSCP Mutation. Используйте форму **no**, чтобы удалить карту Mutation.

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 без пробелов. Максимально допустимое количество символов – 32.
INPUT-DSCP-LIST	Укажите список DSCP, значения которых необходимо «мутировать». Доступный диапазон значений: от 0 до 63. Несколько DSCP могут быть отделены запятой (,) или дефисом (-). Пробелы до и после дефиса недопустимы.
OUTPUT-DSCP	Укажите значение DSCP, которое будет применено после «мутации» Mutation. Доступный диапазон значений: от 0 до 63.

По умолчанию

По умолчанию параметры *OUTPUT-DSCP* и *INPUT-DSCP* равны.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Когда пакет принимается интерфейсом, на основе карты мутации DSCP входящий DSCP может быть мутирован в другой DSCP непосредственно перед любыми операциями QoS. Мутация DSCP полезна для интеграции доменов с различными назначениями DSCP.
При настройке именованной карты мутации DSCP обратите внимание на следующее:

- Введите несколько команд для сопоставления дополнительных значений DSCP с измененным значением DSCP.
- Введите отдельную команду для каждого мутированного значения DSCP.

Карта DSCP-CoS и карта DSCP-цвета по-прежнему будут основаны на исходном DSCP пакета. Все последующие операции будут основаны на измененном DSCP.

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)#
```

61-11 mls qos scheduler

Данная команда используется для настройки механизма обслуживания очередей. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

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.

WDRR 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 ethernet 1/0/1
Switch(config-if)# mls qos scheduler sp
Switch(config-if)#
```

61-12 mls qos trust

Данная команда используется для настройки доверенного статуса (Trust) на порту для поля CoS или DSCP поступающего пакета для последующих QoS-операций. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

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-co**s. 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.

Пакет, полученный портом, будет инициализирован с цветом на основе команды **mls qos map dscp- color** (если на порту настроен статус Trust для DSCP) или с цветом на основе MLS QoS преобразованного CoS (если на порту настроен статус Trust для CoS).

Пример

В данном примере показано, как настроить режим Trust для DSCP на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)#
```

61-13 police

Данная команда используется для настройки Traffic Policing (ограничения трафика) с использованием Single Rate. Используйте форму no, чтобы оменить Traffic Policing.

police *KBPS* **[***BURST-NORMAL* **[***BURST-MAX***]] [conform-action** *ACTION***] exceed-action** *ACTION* **[violate-action** *ACTION***] [color-aware]no police**

Параметры

KBPS	Укажите среднюю скорость в Кбит/с.
BURST-NORMAL	(Опционально) Укажите нормальный размер всплеска (Burst). Единица измерения – Кбайт.
BURST-MAX	(Опционально) Укажите максимальный размер всплеска (Burst). Единица измерения – Кбайт.
conform-action	(Опционально) Укажите, чтобы действие было выполнено к Green Color Packets (пакетам «окрашенным» в зелёный цвет). Если не указано, будет выполнено действие по умолчанию **transmit** (передача пакетов).
exceed-action	Укажите, чтобы действие было выполнено к Yellow Color

	Packets (пакетам, «окрашенным» в желтый цвет), превышающим разрешенную скорость.
violate-action	(Опционально) Укажите, чтобы действие было выполнено к Red Color Packets (пакетам, «окрашенным» в красный цвет). Если данный параметр не указан, используется Single Rate Two Color Policer. Если данный параметр указан, используется Single Rate Three Color Policer.
ACTION	Укажите, чтобы действие было выполнено к пакетам. Ниже указаны ключевые слова: **drop** – отбрасывание пакетов. **set-dscp-transmit** *VALUE* – укажите значение IP DSCP-метки и передачу пакетов с новой IP DSCP-меткой. **set-1p-transmit** – укажите значение 802.1p и передачу пакетов с новым значением. **transmit** – передача пакетов без изменений.
color-aware	(Опционально) Укажите данный параметр для Single Rate Three Color Policer. Если данный параметр не указан, Policer работает в режиме Color Blind. Если данный параметр указан, Policer работает в режиме Color Aware.

По умолчанию

Нет

Режим ввода команды

Policy-map Class Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду **police**, чтобы отбросить или отметить пакеты со значениями QoS, не соответствующими уровню пакета.

Используйте команду **police** *KBPS*, чтобы создать Single Rate Policer. Используйте команду **police cir**, чтобы создать Two Rate Policer. Single Rate Policer может быть Two Color Policer (если указан параметр violate-action) или Three Color Policer (если **violate-action** не указан).

Прибывший на порт пакет будет инициализирован с цветом. Если на получающем порту настроен статус Trust для DSCP, то начальный цвет пакета будет соответствовать входящему DSCP на основе DSCP в карте цветов. Если на получающем порту настроен статус Trust для CoS, то начальный цвет пакета будет соответствовать входящему CoS на основе CoS в карте цветов.

Настроить Single Rate Two Color Policer можно только в режиме Color Blind. В режиме Color Aware может работать как Single Rate Three Color Policer, так и Two Rate Three Color Policer. В режиме Color Blind окончательный цвет пакета определяется только результатом работы policer metering. В режиме Color Aware окончательный цвет пакета определяется начальным цветом пакета и результатом работы policer metering. В данном случае Policer может понизить начальный цвет пакета.

После завершения работы policer metering действие будет выполнено на основе окончательного цвета. Для Green Color Packets применяется действие **conform**, для Yellow Color Packets – действие **exceed**, а для Red Color Packets – **violate**. Действия должны быть согласованы, то есть, например, нельзя указать действие **violate** с **transmit** (передачей) или **exceed** с **drop** (отбрасыванием).

Действия, настроенные в данной команде для класса трафика, будут применены ко всем пакетам, принадлежащим к данному классу трафика.

Пример

В данном примере показано, как настроить класс трафика и критерии соответствия для политики, которую необходимо привязать к настроенному классу трафика в карте политики. Команда **service-policy** используется для привязки данной политики обслуживания к интерфейсу. Traffic Policing настроено для всех входящих пакетах на интерфейсе Ethernet 1/0/1. Настроенная средняя скорость – 8 Кбит/с. Нормальный размер всплеска – 1 Кбайт.

```
Switch# configure terminal
Switch(config)# class-map access-match
Switch(config-cmap)# match access-group name acl_rd
Switch(config-cmap)# exit
Switch(config)# policy-map police-setting
Switch(config-pmap)# class access-match
Switch(config-pmap-c)# police 8 1 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# service-policy input police-setting
Switch(config-if)#
```

61-14 police aggregate

Данная команда используется для настройки Aggregate Policer в качестве политики для класса трафика в карте политик. Используйте форму **no**, чтобы удалить Aggregate Policer из политики класса.

police aggregate *NAME*
no police

Параметры

NAME	Укажите ранее настроенное имя Aggregate Policer в качестве Aggregate Policer для класса трафика.

По умолчанию

Нет

Режим ввода команды

Policy-map Class Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду **mls qos aggregate-policer** в режиме Global Configuration Mode, чтобы создать Aggregate Policer. Затем используйте команду **police aggregate** в режиме Policy-map Class Configuration Mode, чтобы настроить Aggregate Policer в качестве политики для класса трафика. Для разных карт политики настройка общего Aggregate Policer невозможна. Если именованный Aggregate Policer привязан к нескольким входным портам, работа функции Metering будет применена только к трафику, полученному на определенном порту.

Пример

В данном примере показано, как настроить параметры Aggregate Policer и применить его к нескольким классам в карте политики. Имя Aggregate Policer – agg_policer1. Данный Policer создан с использованием Single Rate Policing и настроен в качестве политики для класса трафика 1, 2 и 3.

```
Switch# configure terminal
Switch(config)# mls qos aggregate-policer agg_policer1 10000 16384 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)#
```

61-15 police cir

Данная команда используется для настройки Two-Rate Traffic Policing (CIR и PIR). Используйте форму **no**, чтобы отменить Two-Rate Traffic Policing.

police cir *CIR* **[bc** *CONFORM-BURST***] pir** *PIR* **[be** *PEAK-BURST***] [conform-action** *ACTION***][exceed-action** *ACTION* **][violate-action** *ACTION***]] [color-aware]**
no police

Параметры

CIR	Укажите гарантированную полосу пропускания (Committed Information Rate) в Кбит/с. Данный параметр является первым в алгоритме «корзина маркеров» (Token Bucket) для Two-rate Metering.
PIR	Укажите пиковую скорость передачи (Peak Information Rate) в Кбит/с. Данный параметр является вторым в алгоритме «корзина маркеров» (Token Bucket) для Two-rate Metering.
CONFORM-BURST	(Опционально) Укажите размер всплеска (Burst) для первого параметра алгоритма «корзина маркеров» (Token Bucket). Единица измерения – Кбайт.
PEAK-BURST	(Опционально) Укажите размер всплеска (Burst) для второго параметра алгоритма «корзина маркеров» (Token

	Bucket). Единица измерения – Кбайт.
conform-action	(Опционально) Укажите, чтобы действие было выполнено к Green Color Packets (пакетам, «окрашенным» в зелёный цвет). Если не указано, будет выполнено действие по умолчанию **transmit** (передача пакетов).
exceed-action	(Опционально) Укажите, чтобы действие было выполнено к Yellow Color Packets (пакетам, «окрашенным» в желтый цвет), которые соответствуют PIR, но не соответствуют CIR. Если не указано, будет выполнено действие по умолчанию **drop** (отбрасывание).
violate-action	(Опционально) Укажите, чтобы действие было выполнено к Red Color Packets (пакетам, «окрашенным» в красный цвет), которые не соответствуют CIR и PIR. Если не указано, будет выполнено действие по умолчанию **drop** (отбрасывание).
ACTION	(Опционально) Укажите, чтобы действие было выполнено к пакетам. Ниже указаны ключевые слова: **drop** – отбрасывание пакетов. **set-dscp-transmit** *VALUE* – укажите значение IP DSCP-метки и передачу пакетов с новой IP DSCP-меткой. **set-1p-transmit** – укажите значение 802.1p и передачу пакетов с новым значением. **transmit** – передача пакетов без изменений.
color-aware	(Опционально) Укажите данный параметр для Two Rate Three Color Policer. Если данный параметр не указан, Policer работает в режиме Color Blind. Если данный параметр указан, Policer работает в режиме Color Aware.

По умолчанию

Нет

Режим ввода команды

Policy-map Class Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Прибывший на порт пакет будет инициализирован с цветом. Начальный цвет пакета будет определен в соответствии с DSCP входящего пакета (если на получающем порту настроен статус Trust для DSCP) или в соответствии с CoS входящего пакета (если на получающем порту настроен статус Trust для CoS).

Single Rate Three Color Policer и Two Rate Three Color Policer могут работать в режиме Color Aware. В режиме Color Blind окончательный цвет пакета определяется только результатом работы policer metering. В режиме Color Aware окончательный цвет пакета определяется начальным цветом пакета и результатом работы policer metering. В данном случае Policer может понизить начальный цвет пакета.

После завершения работы policer metering действие будет выполнено на основе окончательного цвета. Для Green Color Packets применяется действие **conform**, для Yellow Color Packets – действие **exceed**, а для Red Color Packets – **violate**. Действия должны быть согласованы, то есть, например, нельзя указать действие **violate** с **transmit** (передача) или **exceed** с **drop** (отбрасыванием).

Действия, настроенные в данной команде для класса трафика, будут применены ко всем пакетам, принадлежащим к данному классу трафика.

Пример

В данном примере показано, как настроить Two-Rate Traffic Policing для класса «police». Для ограничения трафика настроены средняя согласованная скорость 500 Кбит/с и пиковая скорость передачи 1 Мбит/с. Карта политики под именем «policy1» привязана к интерфейсу Ethernet 1/0/3.

```
Switch# configure terminal
Switch(config)# class-map police
Switch(config-cmap)# match access-group name myAcl101
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class police
Switch(config-pmap-c)# police cir 500 bc 10 pir 1000 be 10 exceed-action set-dscp-transmit 2
violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# service-policy output policy1
Switch(config-if)#
```

61-16 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. Используйте форму **no**, чтобы удалить карту политики.

policy-map *NAME*
no policy-map *NAME*

Параметры

NAME	Укажите имя карты политики. Максимально допустимое количество символов – 32.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, 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 00
Switch(config-pmap-c)#
```

61-17 priority-queue cos-map

Данная команда используется для привязки CoS к карте очереди. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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.
COS1	Укажите значение CoS для привязки. Доступный диапазон значений: от 0 до 7.
COS2 ... COS8	(Опционально) Укажите значение CoS для привязки. Доступный диапазон значений: от 0 до 7.

По умолчанию

Привязка приоритета CoS к очереди по умолчанию: 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

Уровень команды по умолчанию

Уровень 12

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)#
```

61-18 queue rate-limit

Данная команда используется для указания/изменения полосы пропускания (Bandwidth), предназначенной для очереди. Используйте форму **no**, чтобы удалить полосу пропускания, предназначенную для очереди.

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. Доступный диапазон значений: от 1 до 100.
MAX PERCENTAGE	Укажите максимальную полосу пропускания в процентах. Доступный диапазон значений: от 1 до 100.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 используется 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» настроены минимальная разрешенная полоса пропускания 100 Кбит/с и максимальная полоса пропускания 2000 Кбит/с. Для очереди 2 «queue 2» настроены минимальная разрешенная полоса пропускания 10% и максимальная полоса пропускания 50%.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# queue 1 rate-limit 100 2000
Switch(config-if)# queue 2 rate-limit percent 10 percent 50
Switch(config-if)#
```

61-19 rate-limit {input | output}

Данная команда используется для настройки значений ограничения полосы пропускания для входящего и исходящего трафика на интерфейсе. Используйте форму **no**, чтобы отменить ограничение полосы пропускания.

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. Доступный диапазон значений: от 1 до 100.
BURST-SIZE	(Опционально) Укажите ограничение для трафика всплеска (Burst). Единица измерения – Кбайт.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Настроенное ограничение не должно превышать максимальную скорость на указанном интерфейсе. Если полученный трафик превышает настроенное 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. Настроенные ограничения входящей полосы пропускания: 2000 Кбит/с и 4096 Кбайт для трафика всплеска (Burst).

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/5
Switch(config-if)# rate-limit input 2000 4096
Switch(config-if)#
```

61-20 service-policy

Данная команда используется для привязки карты политики к типу input или output на интерфейсе. Используйте форму **no**, чтобы удалить политику обслуживания из входящего интерфейса (input).

service-policy input *NAME*
no service-policy input

Параметры

input	Укажите, чтобы привязать карту политики к входящему потоку на интерфейсе.
NAME	Укажите имя карты политики обслуживания. Максимально допустимое количество символов – 32.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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 настроить две карты политики: (1) cust1-classes и (2) cust2-classes. Для cust1-classes: карта класса «gold» настроена для привязки CoS 6 с использованием Single Rate Policer, настроенная согласованная скорость передачи – 800 Кбит/с; карта класса «silver» настроена для привязки CoS 5 с использованием Single Rate Policer, настроенная согласованная скорость передачи – 2000 Кбит/с; карта класса «bronze» настроена для привязки CoS 0 с использованием Single Rate Policer, настроенная согласованная скорость передачи – 8000 Кбит/с.

Для cust2-classes: карта класса «gold» настроена с использованием очереди CoS 6 и Single Rate Policer, настроенная согласованная скорость передачи – 1600 Кбит/с; карта класса «silver» настроена с использованием Single Rate Policer, настроенная согласованная скорость передачи – 4000 Кбит/с; карта класса «bronze» настроена с использованием Single Rate Policer, настроенная согласованная скорость передачи – 16000 Кбит/с.

Настроенная карта политики «cust1-classes» привязана к интерфейсам Ethernet 1/0/1 и 1/0/2 для входящего трафика.

```
Switch# configure terminal
Switch(config)# class-map match-all gold
Switch(config-cmap)# match cos 6
Switch(config-cmap)# exit
Switch(config)# class-map match-all silver
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
Switch(config)# class-map match-all bronze
Switch(config-cmap)# match cos 0
Switch(config-cmap)# exit
Switch(config)# policy-map cust1-classes
Switch(config-pmap)# class gold
Switch(config-pmap-c)# police 800 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver
Switch(config-pmap-c)# police 2000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze
Switch(config-pmap-c)# police 8000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# service-policy input cust1-classes
Switch(config-if)# exit
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# service-policy input cust1-classes
Switch(config-if)#
```

61-21 set

Данная команда используется для настройки полей нового приоритета (Precedence), DSCP и CoS исходящего пакета. Также возможна настройка очереди CoS для пакета.

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. Доступный 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. Доступный 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. Доступный диапазон значений: от 0 до 7. Настройка CoS не повлияет на выбор очереди CoS.
cos-queue *COS-QUEUE*	Укажите очередь CoS для пакетов. Новое значение очереди CoS заменит первоначальное. Очередь CoS не будет назначена, если карта политики привязана к исходящему потоку на интерфейсе.

По умолчанию

Нет

Режим ввода команды

Policy-map Class Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить новое значение полей приоритета (Precedence), DSCP и CoS соответствующих пакетов. Используйте 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. Команды police и set могут быть использованы для одного класса. Команда set применяется к пакетам всех цветов.

Пример

В данном примере показано, как настроить карту политики «policy1» для класса «class1». Пакеты в настроенном классе «class1» будут помечены DSCP 10 с использованием Single Rate Policer, настроенная согласованная скорость передачи – 1 Мбит/с.

```
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)# police 1000000 2000 exceed-action set-dscp-transmit 10
Switch(config-pmap-c)# exit
Switch(config-pmap)#
```

61-22 show class-map

Данная команда используется для отображения настроек карты класса.

show class-map [*NAME***]**

Параметры

NAME	(Опционально) Укажите имя карты класса. Максимально допустимое количество символов – 32.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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 настроенному 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#
```

61-23 show mls qos aggregate-policer

Данная команда используется для отображения настроенного Aggregated Policer.

show mls qos aggregate-policer [*NAME***]**

Параметры

NAME	(Опционально) Укажите имя Aggregated Policer.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить настроенный Aggregated Policer.

Пример

В данном примере показано, как отобразить Aggregated Policer.

```
Switch# show mls qos aggregate-policer

mls qos aggregate-policer agg-policer5 10 1000 conform-action transmit exceed-action drop
mls qos aggregate-policer agg-policer5 cir 500 bc 10 pir 1000 be 10 conform-action transmit
exceed-action set-dscp-transmit 2 violate-action drop

Switch#
```

61-24 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-color | cos-color | dscp-cos}}**

Параметры

interface *INTERFACE-ID*	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-color	Укажите, чтобы отобразить цветовую привязку DSCP.
map cos-color	Укажите, чтобы отобразить цветовую привязку CoS.
map dscp-cos	Укажите, чтобы отобразить привязку DSCP к CoS.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения настроек уровня QoS на указанном интерфейсе.

Пример

В данном примере показано, как отобразить CoS по умолчанию для интерфейсов от Ethernet 1/0/2 до Ethernet 1/0/5.

```
Switch# show mls qos interface ethernet 1/0/2-5 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 данном примере показано, как отобразить статус Trust порта для интерфейсов от Ethernet 1/0/2 до Ethernet 1/0/5.

```
Switch# show mls qos interface ethernet 1/0/2-1/0/5 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 данном примере показано, как отобразить настройки механизма обслуживания очередей для интерфейсов Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch# show mls qos interface ethernet 1/0/1-1/0/2 scheduler

Interface   Scheduler Method
---------- ------------------
eth1/0/1      sp
eth1/0/2      wrr

Switch#
```

В данном 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 ethernet 1/0/1-2 dscp-mutation

Interface   DSCP Mutation Map
---------- ------------------
eth1/0/1       Mutate Map 1
eth1/0/2       Mutate Map 2

Switch#
```

В данном примере показано, как отобразить ограничение полосы пропускания для интерфейсов от Ethernet 1/0/1 до Ethernet 1/0/4.

```
Switch# show mls qos interface ethernet 1/0/1-4 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 данном примере показано, как отобразить ограничение полосы пропускания CoS для интерфейсов Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch# show mls qos interface ethernet 1/0/1-2 queue-rate-limit

eth1/0/1
  QID   Min Bandwidth  Max Bandwidth
  ----  -------------- -------------
  0         -                -
  1         16 kbps          10%(100000 kbps)
  2         32 kbps              -
  3         2%               50%
  4         64 kbps              -
  5         64 kbps              -
  6         32 kbps              -
  7         -                128 kbps
eth1/0/2
  QID   Min Bandwidth  Max Bandwidth
   ----  -------------- -------------
  0         -                -
  1         16 kbps              -
  2         32 kbps              -
  3         32 kbps              -
  4         64 kbps              -
  5         64 kbps              -
  6         32 kbps              -
  7         -                128 kbps

Switch#
```

В данном примере показано, как отобразить цветовую привязку DSCP для интерфейсов Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch# show mls qos interface ethernet 1/0/1-2 map dscp-color

eth1/0/1
  DSCP 0-7 are mapped to green
  DSCP 8-40 are mapped to red
  DSCP 41-43 are mapped to yellow
eth1/0/2
  DSCP 0 - 7 are mapped to green

Switch#
```

В данном примере показано, как отобразить цветовую привязку CoS для интерфейсов Ethernet1/0/3 и Ethernet 1/0/4.

```
Switch# show mls qos interface ethernet 1/0/3-4 map cos-color

eth1/0/3
  CoS 0,1,2 are mapped to green
  CoS 3-4 are mapped to yellow
  CoS 6 are mapped to red
eth1/0/4
  CoS 0,1-6 are mapped to green

Switch#
```

В данном примере показано, как отобразить привязку DSCP к CoS для интерфейса Ethernet 1/0/1.

```
Switch# show mls qos interface ethernet 1/0/1 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 01
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#
```

61-25 show mls qos map dscp-mutation

Данная команда используется для отображения настроек карты QoS DSCP Mutation.

show mls qos maps dscp-mutation [*MAP-NAME*]

Параметры

MAP-NAME	(Опционально) Укажите имя карты DSCP Mutation, которую необходимо отобразить.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется 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: mutation
Attaching interface:
   eth1/0/2-1/0/3,1/0/8-1/0/10

       0  1  2  3  4  5  6  7  8  9
     ---------------------------------
   00  00 10 02 10 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  30 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#
```

61-26 show mls qos queueing

Данная команда используется для отображения информации об очередях QoS и настроек веса (Weight) для разных алгоритмов обслуживания очередей на определенном интерфейсе или интерфейсах.

show mls qos queuing [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально) Укажите ID интерфейса, для которого необходимо отобразить информацию о настройках веса (Weight) разных алгоритмов обслуживания очередей.
,	(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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

При указании ключевого слова **interface**, на определенном интерфейсе или интерфейсах будет отображен настроенный вес для разных алгоритмов обслуживания очередей (WRR или WDRR). 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 данном примере 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#
```

61-27 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 модуль и номер порта.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить политики класса, настроенные для карты политики. Также команда используется для отображения настроек политики класса определенных или всех существующих карт политики обслуживания.

Пример

В этом примере показано, как отобразить карту политики "policy1".

```
Switch# show policy-map policy1

Policy Map policy1
  Class police
police cir 500 bc 10 pir 1000 be 10 conform-action transmit exceed-action set-dscp-
transmit 2 violate-action drop

Switch#
```

В данном примере показано, как отобразить все карты политики на интерфейсе Ethernet 1/0/1.

```
Switch# show policy-map interface eth1/0/1

Policy Map: policy1 : input
  Class police
police cir 500 bc 10 pir 1000 be 10 conform-action transmit exceed-action set-dscp-
transmit 2 violate-action drop

Switch#
```

61-28 wdrr-queue bandwidth

Данная команда используется для настройки значений Quantum для очередей, обслуживаемых механизмом WDRR. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

wdrr-queue bandwidth *QUANTUM1...QUANTUM8*
no wdrr-queue bandwidth

Параметры

QUANTUM1...QUANTUM8	Укажите значение Quantum (число длины кадров) для каждой очереди, обслуживаемой механизмом WDRR.

По умолчанию

Значение Quantum для каждой очереди по умолчанию – 1.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 настроено 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 ethernet 1/0/1
Switch(config-if)# mls qos scheduler wdrr
Switch(config-if)# wdrr-queue bandwidth 1 2 3 4 5 6 7 8
Switch(config-if)#
```

61-29 wrr-queue bandwidth

Данная команда используется для настройки веса (Weight) для очередей, обслуживаемых механизмом WRR. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

wrr-queue bandwidth *WEIGHT1...WEIGHT8*
no wrr-queue bandwidth

Параметры

WEIGHT1...WEIGHT8	Указывает значение веса (количество кадров) для каждой из восьми весовых очередей, используемых в планировании WRR. Диапазон значений веса составляет 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Чтобы использовать 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 настроено 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 ethernet 1/0/1
Switch(config-if)# mls qos scheduler wrr
Switch(config-if)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
Switch(config-if)#
```

62. Команды Remote Network MONitoring (RMON)

62-1 rmon collection stats

Данная команда используется для включения статистики RMON на настраиваемом интерфейсе. Используйте форму **no**, чтобы отключить статистику.

rmon collection stats *INDEX* **[owner** *NAME***]**
no rmon collection stats *INDEX*

Параметры

INDEX	Укажите индекс таблицы RMON. Доступный диапазон значений: от 1 до 65535.
owner *NAME*	Укажите имя владельца. Максимально допустимое количество символов в строке – 127.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 ethernet 1/0/2
Switch(config-if)# rmon collection stats 65 owner guest
Switch(config-if)#
```

62-2 rmon collection history

Данная команда используется для включения сбора истории статистики RMON MIB на настраиваемом интерфейсе. Используйте форму **no**, чтобы отключить сбор истории статистики на интерфейсе.

rmon collection history *INDEX* **[owner** *NAME***] [buckets** *NUM***] [interval** *SECONDS***]**
no rmon collection history *INDEX*

Параметры

INDEX	Укажите индекс таблицы RMON. Доступный диапазон значений: от 1 до 65535.
owner *NAME*	Укажите имя владельца. Максимально допустимое количество символов в строке – 127.
buckets *NUM*	Укажите количество ячеек для сбора истории по группе статистики RMON. Доступный 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). Доступный диапазон значений: от 1 до 3600.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 ethernet 1/0/8
Switch(config-if)# rmon collection history 101 owner it@domain.com interval 2000
Switch(config-if)#
```

62-3 rmon alarm

Данная команда используется для настройки записи уровня alarm (тревога) для мониторинга интерфейса. Используйте форму **no**, чтобы удалить запись уровня alarm.

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. Доступный 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. Доступный 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. Доступный диапазон значений: от 0 до 2147483647.
RISING-EVENT-NUMBER	(Опционально) Укажите индекс записи события, при котором превышено заданное верхнее пороговое значение. Доступный 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. Доступный диапазон значений: от 0 до 2147483647.
FALLING-EVENT-NUMBER	(Опционально) Укажите индекс записи события, при котором достигнуто заданное нижнее пороговое значение. Доступный диапазон значений: от 1 до 65535. Если не указано, никакие действия при достижении нижнего порогового значения не будут применены.
owner *STRING*	(Опционально) Укажите строку владельца. Максимально допустимая длина – 127.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

После настройки RMON alarm будут периодически производится 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)#
```

62-4 rmon event

Данная команда используется для настройки записи события. Используйте форму **no**, чтобы удалить запись события.

rmon event *INDEX* **[log] [[trap** *COMMUNITY***] [owner** *NAME***] [description** *TEXT***]**
no rmon event INDEX

Параметры

INDEX	Укажите индекс записи события. 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. Максимально допустимая длина – 127.
owner *NAME*	Укажите имя владельца. Максимально допустимая длина – 127.
description *TEXT*	(Опционально) Укажите описание для записи события RMON. Максимально допустимое количество символов в строке – 127.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

62-5 show rmon alarm

Данная команда используется для отображения конфигурации alarm.

show rmon alarm

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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#
```

62-6 show rmon events

Данная команда используется для отображения таблицы событий RMON.

show rmon events

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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, 2013-03-02

Event 2, owned by manager2
  Description is Errors
  Event trigger action: log & trap
  Last triggered time:

Switch#
```

62-7 show rmon history

Данная команда используется для отображения информации об истории статистики RMON.

show rmon history

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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 eth4/0/2
  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#
```

62-8 show rmon statistics

Данная команда используется для отображения статистики RMON Ethernet.

show rmon statistics

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить статистику для всех настроенных записей.

Пример

В данном примере показано, как отобразить статистику RMON.

```
Switch# show rmon statistics

Index 32, owned by it@domain.com, Data Source is  eth4/0/3
  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#
```

62-9 snmp-server enable traps rmon

Данная команда используется для включения отправки RMON trap. Используйте форму **no**, чтобы отключить отправку RMON trap.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить/отключить отправку RMON trap.

Пример

В данном 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)#
```

63. Команды Router Advertisement (RA) Guard

63-1 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. Используйте форму **no**, чтобы удалить политику RA Guard Policy.

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

Уровень команды по умолчанию

Уровень 12

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)#
```

63-2 device-role

Данная команда используется для указания роли подключенного устройства. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

device-role {host | router}
no device-role

Параметры

host	Укажите, чтобы настроить подключенное устройство в качестве узла (Host).
router	Укажите, чтобы настроить подключенное устройство в

качестве маршрутизатора (Router).

По умолчанию

Роль по умолчанию – Host.

Режим ввода команды

RA Guard Policy Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

63-3 match ipv6 access-list

Данная команда используется для фильтрации RA-сообщений на основе IPv6-адреса отправителя. Используйте форму **no**, чтобы отключить фильтрацию.

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

Уровень команды по умолчанию

Уровень 12

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)#
```

63-4 ipv6 nd raguard attach-policy

Данная команда используется для применения политики RA Guard Policy на определенном интерфейсе. Используйте форму **no**, чтобы удалить привязку.

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

Уровень команды по умолчанию

Уровень 12

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)#
```

63-5 show ipv6 nd raguard policy

Данная команда используется для отображения информации о политике RA Guard Policy.

show ipv6 nd raguard policy [*POLICY-NAME***]**

Параметры

POLICY-NAME	(Опционально) Укажите имя политики RA Guard Policy.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Если имя политики указано, отображаться будет информация только для указанной политики. Если имя политики не указано, отображаться будет информация для всех политик.

Пример

В данном примере показано, как отобразить конфигурацию политики под именем «raguard1» на всех интерфейсах, на которых применена данная политика.

```
Switch# show ipv6 nd raguard policy raguard1

Policy raguard1 configuration:
      Device Role: host
      Target: eth1/0/1-1/0/2

Switch#
```

64. Команды Safeguard Engine

64-1 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

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#
```

64-2 cpu-protect safeguard

Данная команда используется для включения или настройки функции Safeguard Engine. Используйте форму **no**, чтобы отключить функцию Safeguard Engine.

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. Доступный 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. Доступный диапазон значений: от 20 до 100.

По умолчанию

По умолчанию функция Safeguard Engine отключена.
Верхний порог загрузки ЦПУ по умолчанию – 70.
Нижний порог загрузки ЦПУ по умолчанию – 20.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

64-3 cpu-protect sub-interface

Данная команда используется для настройки пропускной способности (Rate Limit) трафика, предназначенного для ЦПУ по типам под-интерфейсов. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

cpu-protect sub-interface {manage | protocol | route} pps *RATE*

no cpu-protect sub-interface {manage | protocol | route}

Параметры

pps *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

Уровень команды по умолчанию

Уровень 12

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)#
```

64-4 cpu-protect type

Данная команда используется для настройки пропускной способности (Rate Limit) трафика, предназначенного для ЦПУ типом протокола. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

cpu-protect type *PROTOCOL-NAME* **pps** *RATE*
no cpu-protect type *PROTOCOL-NAME*

Параметры

PROTOCOL-NAME	Укажите имя протокола, который необходимо настроить.
pps *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

Уровень команды по умолчанию

Уровень 12

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** – управляющие пакеты протокола, 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 (sub-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
gvrp	GARP VLAN Registration Protocol	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
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 OSPF. Настроенное пороговое значение – 100 пакетов в секунду.

```
Switch# configure terminal
Switch(config)# cpu-protect type ospf pps 100
Switch(config)#
```

64-5 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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   :50%
 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.

64-6 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} [*UNIT-ID***]**

Параметры

UNIT-ID	(Опционально) Укажите идентификатор устройства для отображения конфигурации и статистики ограничения скорости по суб-интерфейсу.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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 : 1000 pps
Unit            Total     Drop
--------------  --------- ---------
1               50        0
3               50        0

Switch#
```

64-7 show cpu-protect type

Данная команда используется для отображения пропускной способности (Rate Limit) и статистики защиты ЦПУ.

show cpu-protect type {*PROTOCOL-NAME* **[***UNIT-ID***] | unit** *UNIT-ID***}**

Параметры

PROTOCOL-NAME	Указывает, что настроенное ограничение скорости и статистика указанного протокола будут отображаться, если не указан дополнительный идентификатор устройства. В противном случае будет отображаться только информация об указанном ID устройства. Параметр UNIT-ID доступен только при включенном режиме стекирования.
unit *UNIT-ID*	Указывает идентификатор устройства для отображения конфигурации и статистики ограничения скорости. Этот параметр доступен только при включенном режиме стекирования.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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: 300  pps
Unit            Total     Drop
--------------  --------- ---------
1               30        0
3               30        0

Switch#
```

64-8 snmp-server enable traps safeguard-engine

Данная команда используется для включения отправки SNMP-уведомлений для Safeguard Engine. Используйте форму **no**, чтобы отключить отправку SNMP-уведомлений для Safeguard Engine.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить/отключить отправку SNMP-уведомлений при изменении текущего режима Safeguard Engine.

Пример

В данном примере показано, как включить отправку trap-сообщений об изменении текущего режима Safeguard Engine.

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

65. Команды Secure Shell (SSH)

65-1 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Данная команда используется 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#
```

65-2 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

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#
```

65-3 ip ssh timeout

Данная команда используется для настройки параметров контроля SSH на коммутаторе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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. Доступный диапазон значений: от 30 до 600.
authentication-retries *NUMBER*	Укажите количество попыток аутентификации. Сессия завершается после всех неудачных попыток. Доступный 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

Уровень команды по умолчанию

Уровень 12

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 SSH на 160 секунд.

```
Switch# configure terminal
Switch(config)# ip ssh timeout 160
Switch(config)#
```

В данном примере показано, как настроить значение попыток аутентификации. Настроенное значение – 2. Соединение будет прервано после 2 неудачных попыток.

```
Switch# configure terminal
Switch(config)# ip ssh authentication-retries 2
Switch(config)#
```

65-4 ip ssh server

Данная команда используется для включения SSH-сервера. Используйте форму **no**, чтобы отключить SSH-сервер.

ip ssh server
no ip ssh server

Параметры

Нет

По умолчанию

По умолчанию SSH-сервер отключен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить SSH-сервер.

Пример

В данном примере показано, как включить SSH-сервер.

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

65-5 ip ssh service-port

Данная команда используется для указания сервисного порта для SSH. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Параметры

TCP-PORT	Укажите номер TCP-порта. Доступный 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

Уровень команды по умолчанию

Уровень 12

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)#
```

65-6 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

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 AAADAQAB AAAAQwCN 6IRFHCBf jsHvYjQG iCL0p2kz 2v38ULC8
kAKra/Ze mG7IW3eC 8STcrkr5 s719H/bh jG/oqkwj S1UJSGqR e/sj6Ws=

Switch#
```

65-7 show ip ssh

Данная команда используется для отображения пользовательских настроек конфигурации SSH.

show ip ssh

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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#
```

65-8 show ssh

Данная команда используется для отображения статуса подключений SSH-сервера.

show ssh

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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/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.

65-9 ssh user authentication-method

Данная команда используется для настройки методов аутентификации SSH для учетной записи пользователя. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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. Максимально допустимое 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. Доступный диапазон значений: от 1 до 255.
IP-ADDESS	(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

Уровень команды по умолчанию

Уровень 15

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. Максимально допустимая 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 user1 authentication-method publickey c:/user1.pub
Switch(config)#
```

66. Команды sFlow

66-1 sflow receiver

Данная команда используется для настройки получателя для агента sFlow. Получатели не могут быть добавлены или удалены из агента sFlow. Используйте форму **no**, чтобы вернуть настройки по умолчанию для одного получателя.

sflow receiver *INDEX* **[owner** *NAME***] [expiry {***SECONDS* **| infinite}] [max-datagram-size** *SIZE***][host {***IP-ADDRESS* **|** *IPV6-ADDRESS***}] [udp-port** *PORT***]**
no sflow receiver *INDEX*

Параметры

INDEX	Укажите индекс получателя.
owner *NAME*	(Опционально) Укажите имя владельца получателя. Максимально допустимое количество символов – 32. При вводе данного параметра строка не должна оставаться пустой.
expiry *SECONDS*	(Опционально) Укажите время истечения записи. Параметр записи будет сброшен после истечения таймера. Доступный диапазон значений: от 0 до 2000000. При вводе данного параметра пользователь не может указать «0» в качестве значения таймера истечения.
infinite	(Опционально) Укажите отсутствие времени истечения записи.
max-datagram-size *SIZE*	(Опционально) Укажите максимальное количество байтов одной дейтаграммы sFlow. Доступный диапазон значений: от 700 до 1400.
host *IP-ADDRESS*	(Опционально) Укажите IPv4-адрес удаленного коллектора sFlow.
host *IPV6-ADDRESS*	(Опционально) Укажите IPv6-адрес удаленного коллектора sFlow.
udp-port *PORT*	(Опционально) Укажите UDP-порт удаленного коллектора sFlow. Значение по умолчанию – 6343. Доступный диапазон значений: от 1 до 65535.

По умолчанию

Строка с именем владельца по умолчанию пустая.
Таймер истечения срока записи по умолчанию – 0 секунд.
Максимальный размер дейтаграммы по умолчанию – 1400 байтов.
IP-адрес получателя по умолчанию – 0.0.0.0.
Номер UDP-порта по умолчанию – 6343.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Агент sFlow имеет фиксированное количество различаемых индексом получателей, созданных системой во время сброса. Эти получатели не могут быть удалены. Владелец записи должен быть настроен перед другими параметрами записи, и только когда запись находится в состоянии сброса (Reset). При вводе команды строка с именем владельца не должна оставаться пустой. Чтобы изменить настроенного владельца, сначала необходимо сбросить его с помощью команды **no sflow receiver**. Получатель будет отключен после окончания его срока действия, а запись получателя вернется к настройкам по умолчанию. Таймер истечения срока записи начинает обратный отсчет после настройки его значения. Пользователь не может указать «0» в качестве значения таймера истечения срока записи.

Пример

В данном примере показано, как настроить получателя с индексом 1. Имя владельца – collector1. Значение тайм-аута – 86400 секунд. Размер – 1400 байтов. IP-адрес удаленного получателя sFlow – 10.1.1.2. Номер порта – 6343.

```
Switch# configure terminal
Switch(config)# sflow receiver 1 owner collector1 expiry 86400 max-datagram-size 1400 host
10.1.1.2 udp-port 6343
Switch(config)#
```

66-2 sflow sampler

Данная команда используется для создания или настройки выборки для агента sFlow. Используйте форму **no**, чтобы удалить одну выборку.

sflow sampler *INSTANCE* **[receiver** *RECEIVER***] [inbound | outbound] [sampling-rate** *RATE***][max-header-size** *SIZE***]**
no sflow sampler *INSTANCE*

Параметры

INSTANCE	Укажите индекс экземпляра, если с одним интерфейсом ассоциировано несколько выборок. Доступный диапазон значений: от 1 до 65535.
receiver *RECEIVER*	(Опционально) Укажите индекс получателя указанной выборки. Если параметр не указан, значение равно нулю. Пользователь не может указать «0» в качестве данного значения.
inbound	(Опционально) Укажите для выборки входящих пакетов. По умолчанию используется данное направление выборки.
outbound	(Опционально) Укажите для выборки исходящих пакетов.
sampling-rate *RATE*	(Опционально) Укажите частоту выборки пакетов. Доступный диапазон значений: от 0 до 65536. Если параметр не указан или указан «0», выборка будет отключена.
max-header-size *SIZE*	(Опционально) Укажите максимальное количество байтов, которое необходимо скопировать из пакетов выборки. Доступный диапазон значений: от 18 до 256. Если параметр

	не указан, значение по умолчанию составляет 128.

По умолчанию

По умолчанию ни одной выборки не создано.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду без ключевых слов, чтобы создать выборку по умолчанию или вернуть значения по умолчанию для существующей выборки. При использовании формы no укажите индекс экземпляра выборки, которую необходимо удалить.

Пользователь может указать только получателя, для которого настроено имя владельца. Если имя владельца получателя сброшено, ассоциированная с ним выборка вернется к настройкам по умолчанию. ID получателя выборки по умолчанию составляет 0.

Возможна настройка двух режимов для экземпляра: inbound или outbound. Если режим не указан, по умолчанию используется inbound, который применяется для контроля входящих пакетов.

На интерфейсе возможна настройка нескольких выборок. Настроенная частота нескольких выборок может отличаться, но частота всех других выборок в одном направлении должна быть кратна минимальной настроенной частоте выборки во второй степени.

Во время перегрузки системы текущая частота выборки может быть автоматически понижена.

Пример

В данном примере показано, как создать выборку экземпляра 1. Получатель – 1. Режим – inbound. Частота – 1024. Размер – 128 байтов.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# sflow sampler 1 receiver 1 inbound sampling-rate 1024 max-header-size 128
Switch(config-if)#
```

66-3 sflow poller

Данная команда используется для создания или настройки опроса для агента sFlow. Используйте форму **no**, чтобы удалить опрос.

sflow poller *INSTANCE* **[receiver** *RECEIVER***] [interval** *SECONDS***]**
no sflow poller *INSTANCE*

Параметры

INSTANCE	Укажите индекс экземпляра, если с одним интерфейсом

	ассоциировано несколько опросов. Доступный диапазон значений: от 1 до 65535.
receiver *RECEIVER*	(Опционально) Укажите индекс получателя указанного опроса. Если параметр не указан, значение равно нулю. Пользователь не может указать «0» в качестве данного значения.
interval *SECONDS*	(Опционально) Укажите максимальное количество секунд между последовательными выборками опроса. Доступный диапазон значений: от 0 до 120. Если параметр не указан или указан «0», опрос будет отключен.

По умолчанию

Опросы по умолчанию не созданы.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду без ключевых слов, чтобы создать опрос по умолчанию или вернуть значения по умолчанию для существующего опроса. При использовании формы no укажите индекс экземпляра опроса, который необходимо удалить.

Пользователь может указать только выборку, для которого настроено имя владельца. Если имя владельца получателя сброшено, ассоциированный с ним опрос вернется к настройкам по умолчанию.

Если для интервала опроса установлено значение 0, опрос будет отключен. На интерфейсе может быть установлено несколько опросов.

Пример

В данном примере показано, как создать опрос экземпляра 1. Получатель – 1. Интервал – 20 секунд.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# sflow poller 1 receiver 1 interval 20
Switch(config-if)#
```

66-4 show sflow

Данная команда используется для отображения информации об sFlow.

show sflow [agent | receiver | sampler | poller]

Параметры

agent	(Опционально) Укажите для отображения информации об

	агенте sFlow.
receiver	(Опционально) Укажите для отображения информации о всех получателях.
sampler	(Опционально) Укажите для отображения информации о всех выборках.
poller	(Опционально) Укажите для отображения информации о всех опросах.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию об sFlow. При отсутствии поддержки MIB, строка sFlow Agent Version с указанием версии MIB будет пустой. При изменении vendor имя организации в строке sFlow Agent Version также будет изменено.

Пример

В данном примере показано, как отобразить информацию о всех типах объектов sFlow.

```
Switch#show sflow

sFlow Agent Version       : 1.3;D-Link Corporation Inc.;1.00
sFlow Agent Address       : 10.90.90.91
sFlow Agent IPv6 Address  :

Receivers Information
Index                     : 1
Owner                     :
Expire Time               : 0
Current Countdown Time    : 0
Max Datagram Size         : 1400
Address                   : 0.0.0.0
Port                      : 6343
Datagram Version          : 5

Index                     : 2
Owner                     :
Expire Time               : 0
Current Countdown Time    : 0
Max Datagram Size         : 1400
Address                   : 0.0.0.0
Port                      : 6343
Datagram Version          : 5

Index                     : 3
Owner                     :
Expire Time               : 0
Current Countdown Time    : 0
Max Datagram Size         : 1400
Address                   : 0.0.0.0
Port                      : 6343
Datagram Version          : 5

Index                     : 4
Owner                     :
Expire Time               : 0
Current Countdown Time    : 0
Max Datagram Size         : 1400
Address                   : 0.0.0.0
Port                      : 6343
Datagram Version          : 5

Samplers Information
Interface Instance Receiver   Mode   Admin Rate  Active Rate  Max Header Size
--------- -------- -------- -------- ----------  -----------  ---------------

Pollers Information
Interface  Instance  Receiver  Interval
---------  --------  --------  --------


Switch#
```

В этом примере показано, как отобразить информацию агента sFlow.

```
Switch# show sflow agent

sFlow Agent Version       : 1.3;D-Link Corporation Inc.;1.00
sFlow Agent Address       : 10.90.90.90
sFlow Agent IPv6 Address  : FE80::201:2FF:FE03:400

Switch#
```

Отображаемые параметры

sFlow Agent Version	Версия MIB, организация и версия программного обеспечения.
sFlow Agent Address	IPv4-адрес агента sFlow.
sFlow Agent IPv6 Address	IPv6-адрес агента sFlow.
Index	Индекс получателей.
Owner	Имя владельца.
Expire Time	Время истечения срока записи, настроенное пользователем.
Current Countdown Time	Время (в секундах), оставшееся до прекращения выборки и опроса.
Max Datagram Size	Максимальное количество байтов одной дейтаграммы sFlow.
Address	IPv4/IPv6-адрес удаленного получателя sFlow.
Port	UDP-порт удаленного получателя sFlow.
Datagram Version	Версия дейтаграммы sFlow.
Interface	Интерфейс, на котором настроена выборка.
Instance	Индекс экземпляра выборки.
Receiver	Индекс получателя для указанной выборки.
Mode	Режимы для экземпляров: inbound, outbound и inactive.
Admin Rate	Частота для выборки пакетов, настроенная пользователем.
Max Header Size	Максимальное количество байтов, которое необходимо скопировать из пакетов выборки.
Interface	Интерфейс, на котором настроен опрос
Instance	Индекс экземпляра опроса.
Receiver	Индекс получателя для указанного опроса.
Interval	Максимальное количество секунд между последовательными опросами.

67. Команды протокола Simple Network Management Protocol (SNMP)

67-1 show snmp trap link-status

Данная команда используется для отображения состояния trap-статуса состояния линии связи (link- status) 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения состояния trap-статуса при обнаружении/разрыве соединения состояния link-up/link-down на интерфейсе.

Пример

В данном примере показано, как отобразить trap-статус состояния link-up/link-down 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        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#
```

67-2 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Для отображения глобальных настроек о состоянии SNMP-сервера используйте команду **show snmp- server**.

Для отображения настроек, касающихся состояния trap, используйте 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 данном примере 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#
```

67-3 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-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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить состояние отправки SNMP trap на порту. Если ни один из опциональных параметров не указан, 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#
```

67-4 snmp-server

Данная команда используется для включения агента SNMP. Используйте форму **no**, чтобы выключить агента SNMP.

snmp-server
no snmp-server

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

67-5 snmp-server contact

Данная команда используется для настройки системной контактной информации для устройства. Используйте форму **no**, чтобы удалить настройки.

snmp-server contact *TEXT*
no snmp-server contact

Параметры

TEXT	(Опционально) Укажите системную контактную информацию. Максимально допустимое количество символов в строке – 255. Пробелы в строке допустимы.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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. Указанная строка – MIS Department II.

```
Switch# configure terminal
Switch(config)# snmp-server contact MIS Department II
Switch(config)#
```

67-6 snmp-server enable traps

Данная команда используется для глобального включения отправки SNMP trap. Используйте форму **no**, чтобы отключить отправку SNMP trap.

snmp-server enable traps
no snmp-server enable traps

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить 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)#
```

67-7 snmp-server enable traps snmp

Данная команда используется для включения отправки всех или определенных SNMP-уведомлений. Используйте форму **no**, чтобы отключить отправку всех или определенных SNMP-уведомлений.

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 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

Уровень команды по умолчанию

Уровень 12

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 данном примере показано, как включить SNMP trap об ошибке аутентификации.

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

67-8 snmp-server location

Данная команда используется для указания информации о системном местоположении. Используйте форму **no**, чтобы удалить настройки.

snmp-server location *TEXT*
no snmp-server location

Параметры

TEXT	Укажите системное местоположение. Максимально допустимое количество символов в строке – 255. Пробелы в строке допустимы.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

67-9 snmp-server name

Данная команда используется для указания информации о системном имени. Используйте форму **no**, чтобы удалить настройки.

snmp-server name *NAME*
no snmp-server name

Параметры

NAME	Укажите имя сервера. Максимально допустимое 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для указания информации о системном имени коммутатора.

Пример

В данном примере показано, как настроить системное имя. Настроенное имя – SiteA-switch.

```
Switch# configure terminal
Switch(config)# snmp-server name SiteA-switch
Switch(config)#
```

67-10 snmp-server trap-sending disable

Данная команда используется для отключения отправки SNMP trap на порту. Используйте форму **no**, чтобы включить отправку SNMP trap на порту.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для отключения отправки 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 с интерфейса Ethernet 1/0/8.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/8
Switch(config-if)# snmp-server trap-sending disable
Switch(config-if)#
```

67-11 snmp-server service-port

Данная команда используется для настройки номера UDP-порта SNMP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

snmp-server service-port *PORT-NUMBER*
no snmp-server service-port

Параметры

PORT-NUMBER	Укажите номер UDP-порта. Доступный диапазон значение: от 1 до 65535. Некоторые номера могут конфликтовать с другими протоколами.

По умолчанию

Номер по умолчанию – 161.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

67-12 snmp-server response broadcast-request

Используйте данную команду, чтобы разрешить серверу отвечать на широковещательные пакеты SNMP GetRequest. Используйте форму **no**, чтобы запретить серверу отвечать на широковещательные пакеты SNMP GetRequest.

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

Уровень команды по умолчанию

Уровень 12

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)#
```

67-13 snmp trap link-status

Данная команда используется для включения отправки уведомлений об обнаружении/разрыве соединения (link-up/link-down), произошедшего на интерфейсе. Используйте форму **no**, чтобы отключить отправку.

snmp trap link-status
no snmp trap link-status

Параметры

Нет

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 ethernet 1/0/1
Switch(config-if)# no snmp trap link-status
Switch(config-if)#
```

67-14 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 о SNMP local engine ID.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

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 данном примере показано, как отобразить информацию об SNMP-сообществе.

```
Switch# show snmp community

Codes: ro - read only, rw - Read Write

Community         access  view
----------------- ---- ------------------------------------------------------
-
System             rw   sales-divison checked with IP access control list:
SalesDvision
public             ro   RD-division checked with IP access control list: HB5
Develop           ro   RD2
private           rw   Line2 checked with IP access control list: HQ

Total Entries: 4

Switch#
```

В данном примере 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 данном примере 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 данном примере 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 данном примере показано, как отобразить SNMP engine ID.

```
Switch# show snmp engineID

Local SNMP engineID: 800000ab033c1e04a1b9e000

Switch#
```

67-15 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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: 000000090200000000C025808
IP access control list:

Total Entries: 2

Switch#
```

67-16 snmp-server community

Данная команда используется для настройки строки идентификатора сообщества (Community String) для доступа к SNMP. Используйте форму **no**, чтобы удалить строку Community String.

snmp-server community [0 | 7] *COMMUNITY-STRING* **[view** *VIEW-NAME***] [ro | rw] [access** *IP-ACL-NAME***] [context** *CONTEXT***]**

no snmp-server community [0 | 7] *COMMUNITY-STRING*

Параметры

0 *COMMUNITY-STRING*	(Опционально) Укажите строку Community String в форме обычного текста. Максимально допустимое количество символов в строке – 32. Данное значение используется по умолчанию.
7 *COMMUNITY-STRING*	(Опционально) Укажите строку Community String в зашифрованном виде.
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.
context *CONTEXT*	(Опционально) Укажите имя SNMP-контекста.

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

Уровень команды по умолчанию

Уровень 15

Использование команды

Данная команда предоставляет простой способ для создания строки Community String для управления SNMPv1 и SNMPv2c. При создании 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)#
```

67-17 snmp-server engineID local

Данная команда используется для указания SNMP engine ID на локальном устройстве. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

snmp-server engineID local *ENGINEID-STRING*
no snmp-server engineID local

Параметры

ENGINEID-STRING	Укажите строку engine ID. Максимально допустимое количество символов в строке – 24.

По умолчанию

По умолчанию SNMP engine ID генерируется автоматически.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

67-18 snmp-server group

Данная команда используется для настройки SNMP-группы. Используйте форму **no**, чтобы удалить SNMP-группу или удалить группу из используемой указанной модели безопасности.

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. Максимально допустимое 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, чтобы пользователь данной группы использовал модель безопасности SNMPv3.
noauth	Укажите для отмены аутентификации и шифрования пакетов.
priv	Укажите для аутентификации и шифрования пакетов.
read *READ-VIEW*	(Опционально) Укажите, чтобы обеспечить доступ на чтение пользователю данной группы.
write *WRITE-VIEW*	(Опционально) Укажите, чтобы обеспечить доступ на запись 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
ReadGroup	SNMPv1	None	CommunityView	None	CommunityView
ReadGroup	SNMPv2c	None	CommunityView	None	CommunityView
WriteGroup	SNMPv1	None	CommunityView	CommunityView	CommunityView
WriteGroup	SNMPv2c	None	CommunityView	CommunityView	CommunityView

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

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 использовать 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)#
```

67-19 snmp-server host

Данная команда используется для указания получателя SNMP-уведомлений. Используйте форму **no**, чтобы удалить получателя.

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***}**

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	Укажите для отмены аутентификации и шифрования пакетов.
priv	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 *PORT-NUMBER*	(Опционально) Укажите номер UDP-порта. Номер UDP-порта trap по умолчанию – 162. Доступный 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

Уровень команды по умолчанию

Уровень 15

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 команд **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 данном примере 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 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. 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)#
```

67-20 snmp-server source-interface traps

Данная команда используется для указания интерфейса, IP-адрес которого будет использован в качестве адреса источника для отправки пакетов SNMP trap. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

snmp-server source-interface traps *INTERFACE-ID*
no snmp-server source-interface traps

Параметры

INTERFACE-ID	Укажите интерфейс, IP-адрес которого будет использован в качестве адреса источника для отправки пакетов SNMP trap.

По умолчанию

По умолчанию используется IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для указания интерфейса, IP-адрес которого будет использован в качестве адреса источника для отправки пакетов SNMP trap.

Пример

В данном примере показано, как настроить VLAN 100 в качестве интерфейса источника для отправки пакетов SNMP trap.

```
Switch# configure terminal
Switch(config)# snmp-server source-interface traps vlan 100
Switch(config)#
```

67-21 snmp-server user

Данная команда используется для создания SNMP-пользователя. Используйте форму **no**, чтобы удалить SNMP-пользователя.

snmp-server user *USER-NAME GROUP-NAME* **{v1| v2c | v3 [encrypted] [auth {md5 | sha}** *AUTH-PASSWORD* **[priv** *PRIV-PASSWORD* **]]} [access** *IP-ACL-NAME***]**

no snmp-server user *USER-NAME GROUP-NAME* **{v1| v2c | v3}**

Параметры

USER-NAME	Укажите имя пользователя. Максимально допустимое количество символов в строке – 32. Пробелы в строке недопустимы.
GROUP-NAME	Укажите имя группы, к которой принадлежит данный пользователь. 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.
encrypted	(Опционально) Укажите для шифрования пароля.
auth	(Опционально) Укажите тип аутентификации.
md5	(Опционально) Укажите использование аутентификации MAC-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	Укажите пароль Private в форме обычного текста. Максимально допустимое количество символов – 64. При указании параметра **encrypted** фиксированная длина пароля – 16 символов.
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

Уровень команды по умолчанию

Уровень 15

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 данном примере 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)#
```

67-22 snmp-server view

Данная команда используется для создания или изменения записи View. Используйте форму no, чтобы удалить указанную запись SNMP View.

snmp-server view *VIEW-NAME OID-TREE* **{included | excluded}**
no snmp-server view *VIEW-NAME*

Параметры

VIEW-NAME	Укажите имя записи View. Доступный 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 SNMPv1, 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

Уровень команды по умолчанию

Уровень 15

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)#
```

68. Команды Single IP Management (SIM)

68-1 sim

Данная команда используется для включения функции Single IP Management. Используйте форму **no**, чтобы отключить функцию Single IP Management.

sim
no sim

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для включения/отключения функции Single IP Management на устройстве.

Пример

В данном примере показано, как включить Single IP Management.

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

68-2 sim role

Данная команда используется для смены роли Candidate Switch на Commander Switch или Commander Switch на Candidate Switch.

sim role {commander [*GROUP-NAME***] | candidate}**

Параметры

commander	Укажите для передачи роли Commander Switch устройству.
GROUP-NAME	(Опционально) Укажите имя группы, назначая устройству роль Commander Switch.
candidate	Укажите для передачи роли Candidate Switch устройству.

По умолчанию

Имя группы Single IP Management по умолчанию – default.
Роль устройства по умолчанию – Candidate Switch.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Технология Single IP Management предусматривает три роли: Candidate Switch и Commander Switch (назначаются пользователем), а также Member Switch (назначается при помощи команды **sim group- member** на Commander Switch).
В SIM-группу входит Commander Switch и множество Member Switch. При смене роли устройства, например, с Commander Switch на Candidate Switch все роли участников SIM-группы будут изменены на Candidate Switch.

Пример

В данном примере показано, как создать SIM-группу.

```
Switch# configure terminal
Switch(config)# sim role commander my-group
Switch(config)#
```

68-3 sim group-member

Данная команда используется для добавления одного Candidate Switch в SIM-группу. Используйте форму **no**, чтобы удалить одного участника из данной SIM-группы.

sim group-member *CANDIDATE-ID* [*PASSWORD*]
no sim group-member *MEMBER-ID*

Параметры

CANDIDATE-ID	Укажите одно устройство в роли Candidate Switch в одной SIM-группе.
PASSWORD	(Опционально) Укажите пароль устройства в роли Candidate Switch.
MEMBER-ID	Укажите одно устройство в роли Member Switch в одной SIM-группе.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

После того как Candidate Switch пройдет аутентификацию 15-уровнего пароля, Commander Switch позволит данному Candidate Switch присоединиться к SIM-группе в качестве Member Switch.

Пример

В данном примере показано, как добавить один Candidate Switch к SIM-группе.

```
Switch# configure terminal
Switch(config)# sim group-member 1 secret
Switch(config)#
```

68-4 sim holdtime

Данная команда используется для настройки времени в секундах параметра Hold-Time. Если устройство (Commander Switch или Candidate Switch) по истечении данного времени не получит сообщения Single IP Management, информация о другом устройстве будет удалена. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

sim holdtime *SECONDS*
no sim holdtime

Параметры

SECONDS	Укажите значение параметра Hold-Time. Доступный диапазон значений: от 100 до 255 секунд.

По умолчанию

Значение по умолчанию – 100 секунд.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

В течение времени удержания, если не было получено сообщение протокола SIM, это произойдет:

- Для переключателя Commander очистить информацию о переключателе Member.
- Для переключателя Member очистить информацию о переключателе Commander и изменить роль на Candidate.

Пример

В данном примере показано, как настроить параметр SIM Hold-Time.

```
Switch# configure terminal
Switch(config)# sim holdtime 120
Switch(config)#
```

68-5 sim interval

Данная команда используется для настройки SIM-интервала в секундах для отправки сообщений протокола Single IP Management. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

sim interval *SECONDS*
no sim interval

Параметры

SECONDS	Укажите значение интервала. Доступный диапазон значений: от 30 до 90 секунд.

По умолчанию

Значение по умолчанию – 30 секунд.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить SIM-интервал в секундах для отправки сообщений протокола Single IP Management.

Пример

В данном примере показано, как настроить интервал для протокола Single IP Management.

```
Switch# configure terminal
Switch(config)# sim interval 60
Switch(config)#
```

68-6 sim management vlan

Данная команда используется для настройки SIM Management VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

sim management vlan *VLAN-ID*
no sim management vlan

Параметры

VLAN-ID	Укажите ID SIM Management VLAN.

По умолчанию

Значение данного параметра по умолчанию – VLAN 1.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Commander Switch и Member Switch SIM-группы отправляют и получают сообщение SIM на SIM Management VLAN.

Пример

В данном примере показано, как настроить SIM Management VLAN. Настроенное значение – 100.

```
Switch# configure terminal
Switch(config)# sim management vlan 100
Switch(config)#
```

68-7 sim remote-config

Данная команда используется для удаленного входа в систему и настройки участника SIM-группы, а также для выхода из удаленной конфигурации.

sim remote-config {member *MEMBER-ID* **| exit}**

Параметры

member *MEMBER-ID*	Укажите логин участника.
exit	Укажите, чтобы выйти из текущей настраиваемой конфигурации участника.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Commander Switch может входить в учетную запись участников SIM-группы и настраивать их при помощи Member ID. Данная команда доступна только на Commander Switch.

Пример

В данном примере показано, как настроить Member ID.

```
Switch# sim remote-config member 1
Switch#
```

68-8 copy sim

Данная команда используется для копирования файлов участникам SIM-группы.

copy sim *SOURCE-URL DESTINATION-URL* **[member** *MEMBER-LIST***]**

Параметры

SOURCE-URL	Укажите URL источника, который необходимо выгрузить на сервер. URL источника находится на Member Switch. Укажите текущую конфигурацию (Running Configuration) в качестве URL источника, чтобы выгрузить ее на TFTP-сервер. Укажите системный журнал (System Log) в качестве URL источника, чтобы выгрузить его на TFTP-сервер.
DESTINATION-URL	Укажите URL назначения для файла, который необходимо загрузить. URL назначения находится на Member Switch. Укажите текущую конфигурацию (Running Configuration) в качестве URL назначения, чтобы загрузить ее с TFTP-сервера на Member Switch. Укажите программное обеспечение (Firmware) в качестве URL назначения, чтобы загрузить его с TFTP-сервера на Member Switch. Загрузочный образ на Member Switch будет заменен загруженным файлом.
member *MEMBER-LIST*	(Опционально) Укажите Member Switch, чтобы загрузить файл. Может быть указано несколько Member Switch одновременно. Для отделения нескольких ID используйте «,»; для отделения диапазона interface ID используйте «-».

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может использоваться на Commander Switch для выгрузки файлов с Member Switch на сервер. Для различия Member Switch ID каждому Member Switch ID будет добавлено имя файла.

Пример

В данном примере показано, как загрузить программное обеспечение (Firmware) на Member Switch 1.

```
Switch# copy sim tftp://10.10.10.58/switch.had firmware member 1

Download firmware 10.10.10.58/ switch.had to member 1 ?(y/n)[n] y

ID   MAC Address       Status
---------------------------------------
1    00-02-01-03-01-03 SUCCESS

Switch#
```

В данном примере показано, как выгрузить системный журнал (System Log) с Member Switch 1.

```
Switch# copy sim system-log tftp: //10.10.10.58/switchlog member 1

Upload system log  from member 1 to 10.10.10.58/switchlog ?(y/n)[n]y

ID   MAC Address       Status
---------------------------------------
1    00-02-01-03-01-03 SUCCESS

Switch#
```

68-9 snmp-server enable traps sim

Данная команда используется для включения отправки trap-сообщений для SIM. Используйте форму **no**, чтобы отключить отправку.

snmp-server enable traps sim
no snmp-server enable traps sim

Параметры

Нет

По умолчанию

По умолчанию функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить/отключить отправку trap-сообщений для SIM.

Пример

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

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

68-10 show sim

Данная команда используется для отображения информации о Single IP Management.

show sim [{candidates [*CANDIDATE-ID***] | members [***MEMBER-ID***] | group [***COMMANDER-MAC***] |neighbor}]**

Параметры

candidates	(Опционально) Укажите, чтобы отобразить информацию обо всех Candidate Switch.
CANDIDATE-ID	(Опционально) Укажите, чтобы отобразить подробную информацию об одном определенном Candidate Switch.
members	(Опционально) Укажите, чтобы отобразить информацию обо всех Member Switch.
MEMBER-ID	(Опционально) Укажите, чтобы отобразить подробную информацию об одном определенном Member Switch.
group	(Опционально) Укажите, чтобы отобразить информацию о других SIM- группах.
COMMANDER-MAC	(Опционально) Укажите, чтобы отобразить подробную информацию об одной определенной группе.
neighbor	(Опционально) Укажите, чтобы отобразить информацию о соседних устройствах.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения информации о Single IP Management.

Пример

В данном примере показано, как отобразить подробную информацию о локальной SIM на Commander Switch.

```
Switch#show sim

    Group Name          : my-group
    SIM Version         : VER-1.61
    Firmware Version    : 1.70.005
    Management VLAN     : 1
    Device Name         : Switch
    MAC Address         : 80-26-89-A5-43-D0
    Platform            : DGS-1510-28XMP
    SIM State           : Enabled
    Role State          : Commander
    Discovery Interval  : 30 sec
    Hold Time           : 100 sec
    Trap                : Enabled

Switch#
```

В данном примере показано, как отобразить подробную информацию о локальной SIM на Member Switch.

```
Switch#show sim

    SIM Version         : VER-1.61
    Firmware Version    : 1.70.005
    Management VLAN     : 1
    Device Name         : Switch
    MAC Address         : F0-7D-68-15-19-28
    Platform            : DGS-1510-28XMP
    SIM State           : Enabled
    Role State          : Member
    Discovery Interval  : 30 sec
    Hold Time           : 100 sec
    ---------------CS Info---------------
    CS Group Name       : my-group
    CS MAC Address      : 80-26-89-A5-43-D0
    CS Hold Time        : 90 s


Switch#
```

В данном примере показано, как отобразить список участников SIM-группы.

```
Switch#show sim members

Member                                                  Hold Firmware
  ID   MAC Address       Platform                       Time Version   Device Name
-------------------------------------------------------------------------------
   1   F0-7D-68-15-19-28 DGS-1510-28P                   90   1.70.005  Switch
   2   F0-7D-68-15-10-28 DGS-1510-28P                   90   1.70.005  Switch

Total Entries: 2

Switch#
```

В данном примере показано, как отобразить подробную информацию об участнике SIM-группы.

```
Switch#show sim members 1

Sim Member Information :

    Member ID             : 1
    Firmware Version      : 1.70.005
    Device Name           : Switch
    MAC Address           : F0-7D-68-15-19-28
    Platform              : DGS-1510-28P
    Hold Time             : 70 sec

Switch#
```

В данном примере показано, как отобразить список Candidate Switch SIM-группы.

```
Switch# show sim candidates

Candidate                                               Hold Firmware
   ID     MAC Address       Platform                    Time Version   Device Name
-------------------------------------------------------------------------------
    1     EE-FF-00-00-12-12 DGS-1510-52                 90   1.70.005  Switch

Total Entries : 1

Switch#
```

В данном примере показано, как отобразить подробную информацию об одном определенном Candidate Switch SIM-группы.

```
Switch# show sim candidates 1

Sim Candidate Infomation :

    Candidate ID       : 1
    Firmware Version   : 1.70.005
    Device Name        : Switch
    MAC Address        : EE-FF-00-00-12-12
    Platform           : DGS-1510-52XMP
    Hold Time          : 100 sec

Switch#
```

В данном примере показано, как отобразить краткую информацию о группе.

```
Switch# show sim group
* means Commander switch

SIM Group Name : default
                                                Hold Firmware
 ID MAC Address       Platform                  Time Version   Device Name
-------------------------------------------------------------------------------
*1  00-02-00-00-08-12 DGS-1510-28P              40   1.70.005  Switch
 2  00-07-15-34-00-50
 3  00-01-02-03-00-10

SIM Group Name : SIM2
                                                Hold Firmware
 ID MAC Address       Platform                  Time Version   Device Name
-------------------------------------------------------------------------------
*1  00-01-02-03-04-11 DGS-1510-28P              40   1.70.005  Switch
 2  00-55-55-00-55-11

Total Entries : 2

Switch#
```

В данном примере показано, как отобразить подробную информацию о группе.

```
Switch# show sim group 00-02-00-00-08-12

Sim Group Information :

    [*** Commander Info ***]

    MAC Address           : 00-02-00-00-08-12
    Group Name            : default
    Device Name           : Switch
    Firmware Version      : 1.70.005
    Platform              : DGS-1510-28XMP
    Number of Members     : 2
    Hold Time             : 100 sec

    [*** Member Info (1/2)***]

    MAC Address    : 00-07-15-34-00-50

    [*** Member Info (2/2)***]

    MAC Address    : 00-01-02-03-00-10

Switch#
```

В данном примере показано, как отобразить краткую информацию о соседних устройствах SIM- группы.

```
Switch# show sim neighbor

Port       MAC Address        Role
-------------------------------------
eth1/0/1   00-02-00-00-08-12  Member
eth1/0/2   00-01-00-00-12-12  Member
eth1/0/2   EE-FF-00-00-12-12  Candidate

Total Entries : 3

Switch#
```

69. Команды Spanning Tree Protocol (STP)

69-1 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-ID	Укажите интерфейс порта, на котором необходимо запустить действие обнаружения.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

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#
```

69-2 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, 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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#
```

69-3 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, 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду для отображения настроек интерфейса Spanning Tree. Команда может быть использована 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 ethernet 1/0/1

eth1/0/1
 Spanning tree state : Enabled
 Port path cost: 0
 Port priority: 128
 Port Identifier:  128.1
 Link type: auto
 Port fast: edge
 Guard root: Disabled
 TCN filter : Disabled
 Bpdu forward: Disabled

Switch#
```

69-4 snmp-server enable traps stp

Данная команда используется для включения отправки SNMP-уведомлений для STP. Используйте форму **no**, чтобы отключить отправку уведомлений для STP.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить/отключить отправку trap-уведомлений. Если ни один из опциональных параметров не указан в форме **no** данной команды, 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)#
```

69-5 spanning-tree global state

Данная команда используется для включения/отключения глобального состояния STP. Используйте форму **no**, чтобы отключить глобальное состояние STP.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду в режиме Global Configuration Mode, чтобы включить 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)#
```

69-6 spanning-tree (timers)

Данная команда используется для настройки значений таймеров Spanning Tree. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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. Доступный 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. Доступный диапазон значений: от 4 до 30 секунд.
max-age *SECONDS*	Укажите максимальное время жизни сообщения BDPU. Доступный 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

Уровень команды по умолчанию

Уровень 12

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)#
```

69-7 spanning-tree state

Данная команда используется для включения /отключения STP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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 эта функция включена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 ethernet 1/0/1
Switch(config-if)# spanning-tree state enable
Switch(config-if)#
```

69-8 spanning-tree cost

Данная команда используется для настройки значения стоимости пути на указанном порту. Используйте форму **no**, чтобы определить стоимость пути автоматически.

spanning-tree cost *COST*
no spanning-tree cost

Параметры

COST	Укажите стоимость пути для порта. Доступный 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

Уровень команды по умолчанию

Уровень 12

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. Настроенное значение: 20000.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/7
Switch(config-if)# spanning-tree cost 20000
Switch(config-if)#
```

69-9 spanning-tree guard root

Данная команда используется для включения функции STP Root Guard. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

spanning-tree guard root
no spanning-tree guard root

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 ethernet 1/0/1
Switch(config-if)# spanning-tree guard root
Switch(config-if)#
```

69-10 spanning-tree link-type

Данная команда используется для настройки типа соединения (Link-type) для порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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 ни один из параметров не указан, тип соединения по умолчанию назначается на основе настроек дуплекса.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

На портах, функционирующих в режиме полного дуплекса, устанавливается соединение Point To Point; 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 Link-type модулем STP.

Данные настройки действительны для всех режимов Spanning Tree.

Пример

В данном примере показано, как настроить тип соединения Point To Point для Ethernet-порта 1/0/7.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/7
Switch(config-if)# spanning-tree link-type point-to-point
Switch(config-if)#
```

69-11 spanning-tree mode

Данная команда используется для настройки режима STP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

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 Discarding (отбрасывание).

Пример

В данном примере показано, как настроить текущую версию протокола STP на RSTP.

```
Switch# configure terminal
Switch(config)# spanning-tree mode rstp
Switch(config)#
```

69-12 spanning-tree portfast

Данная команда используется для настройки режима Port Fast на порту. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

spanning-tree portfast {disable | edge| network}
no spanning-tree portfast

Параметры

disable	Укажите для включения режима Fast Disable на порту.
edge	Укажите для включения режима Fast Edge на порту.
network	Укажите для включения режима Fast Network на порту.

По умолчанию

Режим по умолчанию – Edge Mode.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

На порту может быть установлен один из трех режимов Port Fast:

- **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 для Ethernet-порта 1/0/7.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/7
Switch(config-if)# spanning-tree portfast edge
Switch(config-if)#
```

69-13 spanning-tree port-priority

Данная команда используется для настройки значения приоритета STP на указанном порту. Команда применима только для версий RSTP и STP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

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 Ethernet-порта 1/0/7 со значением 0.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/7
Switch(config-if)# spanning-tree port-priority 0
Switch(config-if)#
```

69-14 spanning-tree priority

Данная команда используется для настройки приоритета моста. Команда применима только для версий RSTP и STP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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. Доступный диапазон значений: от 0 до 61440.

По умолчанию

Значение по умолчанию – 32768.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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)#
```

69-15 spanning-tree tcnfilter

Данная команда используется для включения фильтрации уведомлений об изменении топологии сети TCN (Topology Change Notification) на указанном интерфейсе. Используйте форму **no**, чтобы отключить фильтрацию TCN.

spanning-tree tcnfilter
no spanning-tree tcnfilter

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 Ethernet-порту 1/0/7.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/7
Switch(config-if)# spanning-tree tcnfilter
Switch(config-if)#
```

69-16 spanning-tree tx-hold-count

Данная команда используется для ограничения максимального количества BPDU, которые могут быть отправлены перед паузой в одну секунду. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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. Доступный диапазон значений: от 1 до 10.

По умолчанию

Значение по умолчанию – 6.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12
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)#
```

69-17 spanning-tree forward-bpdu

Данная команда используется для включения BDPU Forwarding в Spanning Tree. Используйте форму **no**, чтобы отключить BDPU Forwarding в Spanning Tree.

spanning-tree forward-bpdu
no spanning-tree forward-bpdu

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 ethernet 1/0/2
Switch(config-if)# spanning-tree forward-bpdu
Switch(config-if)#
```

70. Команды стекирования

70-1 stack

Данная команда используется для включения функции линейного стекирования. Используйте форму **no**, чтобы отключить функцию линейного стекирования.

stack
no stack

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Порты стекируемого коммутатора, используемые для объединения в цепочку с другими коммутаторами, могут работать как стекирующие порты или как обычные порты Ethernet в зависимости от настройки команды стека. Настройка команды стека в коммутационном блоке должна быть включена до того, как коммутационный блок можно будет объединить в цепочку с другими коммутационными блоками. Настройка будет сохранена в отдельном коммутационном блоке, если пользователь сохранит конфигурацию.

Пример

В данном примере показано, как включить режим стекирования.

```
Switch#stack

 WARNING: The command does not take effect until the next reboot.
Switch#
```

70-2 stack renumber

Данная команда используется для назначения Unit ID коммутатору вручную. Используйте форму **no**, чтобы назначить Unit ID коммутатору автоматически.

stack *CURRENT-UNIT-ID* **renumber** *NEW-UNIT-ID*
no stack *CURRENT-UNIT-ID* **renumber**

Параметры

CURRENT-UNIT-ID	Укажите текущий Unit ID коммутатора.
NEW-UNIT-ID	Укажите новый Unit ID, который необходимо назначить коммутатору.

По умолчанию

По умолчанию Unit ID назначается автоматически.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Изначально у коммутатора отсутствует Unit ID. При инициализации или добавлении в стек коммутатора Unit ID будет автоматически назначен основным устройством (Master). Unit ID можно сохранить в конфигурационном файле после его назначения, применив команду **copy running-config startup-config**. Сохранившийся Unit ID будет использован при следующем запуске устройства.

Используйте данную команду для переназначения Unit ID указанного коммутатора. Назначенный Unit ID будет использован при следующем запуске устройства.

При автоматическом назначении Unit ID основным устройством (Master) применяются следующие правила:

- Unit ID основного устройства (Master) при автоматическом назначении – 1.
- Коммутатор не будет добавлен в стек при обнаружении конфликта его Unit ID с существующим Unit ID.

Пример

В данном примере показано, как изменить Unit ID коммутатора. Прежний ID – 2. Новый ID – 3.

```
Switch# stack 2 renumber 3

 WARNING: The command does not take effect until the next reboot.
Switch#
```

70-3 stack priority

Данная команда используется для настройки приоритета коммутатора в стеке. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

stack *CURRENT-UNIT-ID* **priority** *NEW-PRIORITY-NUMBER*
no stack *CURRENT-UNIT-ID* **priority**

Параметры

CURRENT-UNIT-ID	Укажите текущий Unit ID коммутатора.

NEW-PRIORITY-NUMBER	Укажите приоритет, который необходимо назначить Unit коммутатора в стеке. Доступный диапазон значений: от 1 до 63. Чем меньше номер, тем выше приоритет.

По умолчанию

Значение по умолчанию – 32.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для настройки приоритета указанного коммутатора. Среди коммутаторов, объединенных в стек линейной топологии, основным устройством (Master) становится коммутатор с наивысшим приоритетом. Следующий по приоритету коммутатор будет выбран в качестве резервного устройства (Backup master). Чем меньше значение, тем выше приоритет. Если приоритеты коммутаторов равны, высший приоритет получает коммутатор с наименьшим значением MAC-адреса. При необходимости настройки могут быть сохранены в отдельном Unit.

Пример

В данном примере показано, как настроить приоритет Unit 2 коммутатора со значением 10.

```
Switch# stack 2 priority 10
Switch#
```

70-4 stack preempt

Данная команда используется для включения функции Preempt, с помощью которой можно присвоить роль основного устройства (Master) коммутатору, который будет добавлен в стек, если его приоритет выше, чем у текущего основного устройства. Используйте форму **no**, чтобы отключить функцию Preempt.

stack preempt
no stack preempt

Параметры

Нет

По умолчанию

По умолчанию функция включена.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если функция Preempt отключена, роль основного устройства (Master) не будет присвоена коммутатору, который будет добавлен в стек, даже если его приоритет выше, чем у текущего основного устройства. Если функция Preempt включена, то роль основного устройства (Master) будет присвоена коммутатору, который будет добавлен в стек, если его приоритет выше, чем у текущего основного устройства.

Пример

В данном примере показано, как включить функцию Preempt.

```
Switch# stack preepmt
Switch#
```

70-5 snmp-server enable traps stack

Данная команда используется для включения отправки trap-сообщений, касающихся стекирования. Используйте форму **no**, чтобы отключить отправку trap-сообщений, касающихся стекирования.

snmp-server enable traps stack
no snmp-server enable traps stack

Параметры

Нет

По умолчанию

По умолчанию функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить/отключить отправку SNMP-уведомлений, касающихся стекирования.

Пример

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

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

Switch(config)#
```

70-6 show stack

Данная команда используется для отображения информации о стекировании.

show stack

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию о стекировании.

Пример

В данном примере показано, как отобразить информацию о стекировании.

```
Switch#show stack

Stacking Mode        : Enabled
Stack Preempt        : Enabled
Trap State           : Disabled

Topology             : Duplex_Chain
My Box ID            : 1
Master ID            : 1
BK Master ID         : 2
Box Count            : 2

Box User Module               Prio-                    Prom     Runtime  H/W
ID  Set  Name           Exist rity  MAC                Version  Version  Version
--- ---- -------------- ----- ----- ------------------ -------- -------- -------
1   Auto DGS-1510-28XMP Exist 32    3C-1E-04-A1-B9-E0 1.00.016 1.70.005 A1
2   Auto DGS-1510-28P   Exist 32    F0-7D-68-15-19-28 1.00.016 1.70.005 A1
3   -    NOT_EXIST      No
4   -    NOT_EXIST      No
5   -    NOT_EXIST      No
6   -    NOT_EXIST      No

Switch#
```

71. Команды Storm Control

71-1 snmp-server enable traps storm-control

Данная команда используется для включения и настройки отправки SNMP-уведомлений для Storm Control. Используйте форму **no**, чтобы отключить отправку SNMP-уведомлений.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения и настройки отправки SNMP-уведомлений для Storm Control.

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)#
```

71-2 storm-control

Данная команда используется для защиты устройства от штормовых атак широковещательных и многоадресных пакетов или пакетов с неизвестным адресом назначения. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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. Доступный диапазон значений: от 1 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. Доступный диапазон значений: от 1 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. Доступный диапазон значений: от 1 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

Storm Control широковещательной, многоадресной и одноадресной (DLF) рассылки по умолчанию отключен.

При возникновении шторма по умолчанию Storm пакеты будут отброшены.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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.

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 3,2 установлен порог до 70% с действием отбрасывания (Drop).

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# storm-control broadcast level pps 500
Switch(config-if)# storm-control action shutdown
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# storm-control broadcast level 70 60
Switch(config-if)# storm-control action drop
Switch(config-if)#
```

71-3 storm-control polling

Данная команда используется для настройки интервала опроса (Polling Interval) для подсчета количества полученных пакетов. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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. Доступный диапазон значений: от 1 до 300 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. Доступный 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать интервал выборки для подсчета количества полученных пакетов.

Пример

В данном примере показано, как указать интервал опроса на 15 секунд.

```
Switch# configure terminal
Switch(config)# storm-control polling interval 15
Switch(config)#
```

71-4 show storm-control

Данная команда используется для отображения текущих настроек функции Storm Control.

show storm-control interface *INTERFACE-ID* **[, | -] [broadcast | multicast | unicast]**

Параметры

interface *INTERFACE-ID*	Укажите интервал опроса для подсчета количества полученных пакетов. Доступный диапазон значений: от 1 до 300 секунд.
,	(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.
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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Если ID интерфейса не указан, будут отображены настройки всех интерфейсов. 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.

```
Switch# show storm-control interface ethernet 1/0/1-1/0/6 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 %            70 %       Dropped
eth1/0/4     Shutdown  60/50 %            20 %       Forwarding
eth1/0/5     None      60000/50000 kbps   2000 kbps  Forwarding
eth1/0/6     None      -                  -          Inactive

Total Entries: 6

Switch#
```

В этом примере показано, как отобразить все типы настроек управления штормом на портах 1 - 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.

72. Команды Surveillance VLAN

72-1 surveillance vlan

Данная команда используется для глобального включения функции Surveillance VLAN и ее настройки. Используйте форму **no**, чтобы отключить функцию Surveillance VLAN.

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

Уровень команды по умолчанию

Уровень 12

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.

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 член 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.

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)#
```

72-2 surveillance vlan aging

Данная команда используется для настройки времени устаревания (Aging Time) для устаревших динамических Member-портов Surveillance VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для настройки времени устаревания для устройства 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 на 30 минут.

```
Switch# configure terminal
Switch(config)#surveillance vlan aging 30
Switch(config)#
```

72-3 surveillance vlan enable

Данная команда используется для включения функции Surveillance VLAN на портах. Используйте форму **no**, чтобы отключить функцию Surveillance VLAN на портах.

surveillance vlan enable
no surveillance vlan enable

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда доступна для настройки интерфейсов физического порта и port-channel. Команда используется 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 член 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 физическом порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#surveillance vlan enable
Switch(config-if)#
```

72-4 surveillance vlan mac-address

Данная команда используется для добавления уникального идентификатора организации (OUI), определяемого с устройства системы видеонаблюдения в Surveillance VLAN. Используйте форму **no**, чтобы удалить OUI устройства Surveillance.

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. Максимально допустимое количество символов – 32.

По умолчанию

OUI Address	Mask	Component Type	Description
28-10-7B-00-00-00	FF-FF-FF-E0-00-00	T-COM Device	IP Surveillance Device
Device 28-10-7B-20-00-00	FF-FF-FF-F0-00-00	T-COM Device	IP Surveillance Device
Device B0-C5-54-00-00-00	FF-FF-FF-80-00-00	T-COM Device	IP Surveillance Device
Device F0-7D-68-00-00-00	FF-FF-FF-F0-00-00	T-COM Device	IP Surveillance Device

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для добавления одного или нескольких OUI Surveillance VLAN. OUI используется 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)#
```

72-5 surveillance vlan onvif-discover-port

Эта команда используется для настройки номера порта TCP/UDP для обнаружения потоков RTSP.
Используйте **no** для возврата к настройкам по умолчанию.

surveillance vlan onvif-discover-port *VALUE*
no surveillance vlan onvif-discover-port

Параметры

VALUE	Введите здесь номер порта TCP/UDP. Диапазон может быть либо 554, либо от 1025 до 65535.

По умолчанию

По умолчанию это значение равно 554.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для настройки номера порта TCP/UDP для обнаружения потоков RTSP. IPC с поддержкой ONVIF и NVR с поддержкой ONVIF используют WS-Discovery для поиска других устройств. После обнаружения IPC коммутатор может обнаружить NVR, прослушивая пакеты RTSP, HTTP и HTTPS между NVR и IPC. Эти пакеты нельзя прослушивать, если порт TCP/UDP не равен номеру порта RTSP.

Пример

В этом примере показано, как настроить номер порта TCP/UDP на 2000 для обнаружения потока RTSP.

```
Switch# configure terminal
Switch(config)# surveillance vlan onvif-discover-port 2000
Switch(config)#
```

72-6 surveillance vlan onvif-ipc state

Эта команда используется для настройки состояния IPC распознавания ONVIF. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

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	Введите здесь IP-адрес IPC.
MAC-ADDRESS	(Опционально) Введите MAC-адрес IPC, который распознается с помощью ONVIF.
enable	Указывает, что состояние ONVIF recognition IPC будет включено.
disable	Указывает, что состояние ONVIF recognition IPC будет отключено.

По умолчанию

По умолчанию эта функция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки состояния IPC для распознавания ONVIF с указанием только IP-адреса IPC или IP- и MAC-адреса IPC. Когда IPC ONVIF распознан, можно настроить состояние для указанного устройства. Если имеется более одного IPC с одинаковым IP-адресом и MAC-адреса этих IPC не указаны, состояние этих IPC будет затронуто.

Эта функция используется для блокировки трафика IPC или нет. Если состояние IPC на порту отключено, трафик от IPC будет заблокирован.

Пример

В этом примере показано, как включить режим IPC с IP-адресом 172.18.60.1.

```
Switch# configure terminal
Switch(config)# surveillance vlan onvif-ipc 172.18.60.1 state enable
Switch(config)#
```

72-7 surveillance vlan onvif-ipc description

Эта команда используется для настройки описания IPC, распознаваемого ONVIF. Используйте команду **no** для удаления описания.

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	Введите здесь IP-адрес IPC, признанного ONVIF.
MAC-ADDRESS	(Опционально) Введите MAC-адрес IPC, который распознается с помощью ONVIF.
enable	Введите здесь описание IPC, признанного ONVIF. Оно может содержать до 32 символов.

По умолчанию

По умолчанию для IPC, признанного ONVIF, не определено описание.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для настройки описания IPC, признанного ONVIF, с указанием только IP-адреса IPC или IP- и MAC-адреса IPC. Если имеется несколько IPC с одинаковым IP-адресом и MAC-адреса этих IPC не указаны, будет настроено описание этих IPC.

Пример

В этом примере показано, как определить описание IPC с IP-адресом 172.18.60.1 как 'ipc1'.

```
Switch# configure terminal
Switch(config)# surveillance vlan onvif-ipc 172.18.60.1 description ipc1
Switch(config)#
```

72-8 surveillance vlan onvif-nvr description

Эта команда используется для настройки описания NVR с поддержкой ONVIF. Используйте команду **no** для удаления этого описания.

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	Введите здесь IP-адрес сетевого видеорегистратора с поддержкой ONVIF.
MAC-ADDRESS	(Опционально) Введите MAC-адрес сетевого видеорегистратора, который распознается с помощью ONVIF.
enable	Введите здесь описание сетевого видеорегистратора с поддержкой ONVIF. Он может содержать до 32 символов.

По умолчанию

По умолчанию для NVR, признанного ONVIF, не определено описание.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Когда сетевой видеорегистратор ONVIF распознан, можно настроить описание для указанного устройства.

Эта команда используется для настройки описания распознанного ONVIF NVR с указанием только IP-адреса NVR или IP- и MAC-адреса NVR. Если существует несколько NVR с одинаковым IP-адресом, а MAC-адреса этих NVR не указаны, будет настроено описание этих NVR.

Пример

В этом примере показано, как определить описание сетевого видеорегистратора с IP-адресом 172.18.60.2 как 'nvr1'.

```
Switch# configure terminal
Switch(config)# surveillance vlan onvif-nvr 172.18.60.2 description nvr1
Switch(config)#
```

72-9 surveillance vlan qos

Эта команда используется для настройки приоритета CoS для входящего трафика VLAN наблюдения. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

surveillance vlan qos *COS-VALUE*
no surveillance vlan qos

Параметры

COS-VALUE	Указывает приоритет сети наблюдения VLAN. Доступное значение - от 0 до 7.

По умолчанию

Значение по умолчанию 5.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Пакеты наблюдения, поступающие на порт с включенной ВЛВС наблюдения, помечаются COS, указанным командой.
Пометка COS позволяет отличить трафик VLAN наблюдения от трафика данных по качеству обслуживания.

Пример

В этом примере показано, как настроить приоритет VLAN наблюдения на 7.

```
Switch# configure terminal
Switch(config)# surveillance vlan qos 7
Switch(config)#
```

72-10 show surveillance vlan

Эта команда используется для отображения конфигураций VLAN наблюдения.

show surveillance vlan [interface [*INTERFACE-ID* **[, | -]]]**
show surveillance vlan device [interface [*INTERFACE-ID* **[, | -]]]**

Параметры

device	Указывает для отображения информации об изученных устройствах наблюдения.
interface	(Опционально) Указывает на отображение информации о VLAN наблюдения для портов.
INTERFACE-ID	(Опционально) Укажите порт, который будет отображаться.
,	(Опционально) Указывает серию интерфейсов или отделяет диапазон интерфейсов от предыдущего диапазона. До или после запятой пробел не допускается.
-	(Опционально) Указывает диапазон интерфейсов. До и после дефиса пробел не допускается.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду для отображения конфигураций сети наблюдения VLAN.

Команда **show surveillance vlan** используется для отображения глобальных конфигураций сети наблюдения VLAN.

Команда **show surveillance vlan interface** используется для отображения конфигураций vlan наблюдения на интерфейсах.

Команда **show surveillance vlan device** используется для отображения устройства наблюдения, обнаруженного по его OUI.

Пример

В этом примере показано, как отобразить глобальные настройки сети наблюдения 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#
```

72-11 show surveillance vlan onvif-ipc interface

Эта команда используется для отображения информации IPC на основе ONVIF.

show surveillance vlan onvif-ipc interface [*INTERFACE-ID* **[, | -]] {brief | detail}**

Параметры

INTERFACE-ID	(Опционально) Укажите порт, который будет отображаться.
,	(Опционально) Указывает серию интерфейсов или отделяет диапазон интерфейсов от предыдущего диапазона. До или после запятой пробел не допускается.
-	(Опционально) Указывает диапазон интерфейсов. До и после дефиса пробел не допускается.
brief	Указывает на отображение краткой информации об IP-камере на основе ONVIF.
detail	Указывает на отображение подробной информации об IP-камере на базе ONVIF.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Эта команда используется для отображения краткой или подробной информации IPC на основе ONVIF.

Пример

В этом примере показано, как отобразить краткую информацию об IP-камере на базе 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 этом примере показано, как отобразить подробную информацию об IP-камере на базе ONVIF.

```
Switch# show surveillance vlan onvif-ipc interface ethernet 1/0/1 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#
```

72-12 show surveillance vlan onvif-nvr interface

Эта команда используется для отображения информации о NVR и группах на базе ONVIF.

show surveillance vlan onvif-nvr interface [*INTERFACE-ID* **[, | -]] [ipc-list]**

Параметры

INTERFACE-ID	(Опционально) Указывает порт для отображения.
,	(Опционально) Указывает серию интерфейсов или отделяет диапазон интерфейсов от предыдущего диапазона. До или после запятой пробел не допускается.
-	(Опционально) Указывает диапазон интерфейсов. До и после дефиса пробел не допускается.
ipc-list	(Опционально) Указывает для отображения информации о группе NVR.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Эта команда используется для отображения информации о NVR и группе на базе ONVIF. ID группы - это ID группы IPC, которые принадлежат группе NVR. NVR и управляемые им IPC должны иметь одинаковый идентификатор группы.

Пример

В этом примере показано, как отобразить информацию о NVR на базе ONVIF.

```
Switch# show surveillance vlan onvif-nvr interface ethernet 1/0/1

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 этом примере показано, как отобразить информацию о NVR на базе ONVIF, связанную с идентификатором группы 'ipc- list'.

```
Switch# show surveillance vlan onvif-nvr interface ethernet 1/0/1 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#
```

73. Команды портов коммутатора

73-1 duplex

Эта команда используется для настройки duplex интерфейса физического порта. Используйте форму **no** для возврата к настройкам по умолчанию.

duplex {full | half | auto}
no duplex

Параметры

full	Укажите для работы порта в режиме полного дуплекса (Full-Duplex Mode).
half	Указывает, что порт работает в полудуплексном режиме.
auto	Укажите, чтобы режим дуплекса на порту был определен автосогласованием (Auto-Negotiation).

По умолчанию

Для интерфейсов 100Base-TX и 1000Base-T параметр по умолчанию – **auto**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Для модулей 1000BASE-T, если скорость установлена на 1000, то дуплексный режим не может быть установлен на полудуплексный. Если дуплексный режим установлен на полудуплекс, то скорость не может быть установлена на 1000.

Автосогласование будет включено, если для параметра скорости установлено значение auto или для параметра дуплекса установлено значение auto. Если параметр скорости установлен на auto, а параметр дуплекса установлен на фиксированный режим, будет согласована только скорость. Объявленные возможности будут настроены на дуплексный режим в сочетании со всеми возможными скоростями. Если скорость установлена на фиксированную скорость, а дуплекс установлен на auto, согласовывается только режим дуплекса. Рекламируемые возможности будут включать в себя как полнодуплексный, так и полудуплексный режим в сочетании с настроенными скоростями.

Пример

В этом примере показано, как настроить порт 1 для работы на принудительной скорости 100 Мбит и указать, что дуплексный режим должен быть установлен на auto-negotiated.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# speed 100
Switch(config-if)# duplex auto
Switch(config-if)#
```

73-2 flowcontrol

Данная команда используется для настройки возможности управления потоком (Flow Control) на интерфейсе порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

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.

Данная команда не поддерживается коммутаторами, объединенными в физический стек.

Пример

В данном примере показано, как включить управление потоком на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# flowcontrol on
Switch(config-if)#
```

73-3 mdix

Данная команда используется для настройки состояния MDIX порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Режим по умолчанию – Auto.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 ethernet 1/0/1
Switch(config-if)#mdix auto
Switch(config-if)#
```

73-4 speed

Данная команда используется для настройки скорости интерфейса физического порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

speed {10 | 100 | 1000 [master | slave] | 10giga [master | slave] | auto [*SPEED-LIST***]} [rj45 | sfp]**
no speed [rj45 | sfp]

Параметры

10	Укажите, чтобы установить скорость 10 Мбит/с.
100	Укажите, чтобы установить скорость 100 Мбит/с.
1000	Укажите, чтобы установить скорость 1000 Мбит/с на медных портах. Необходимо вручную задать статус порта: Master (основное устройство) или Slave (дополнительное устройство). Укажите, чтобы отключить автосогласование на всех оптических портах (1000Base-SX/LX).
master | slave	Укажите статус порта: Master (основное устройство) или Slave (дополнительное устройство). Данный параметр применим только к устройствам, подключенным к порту 1000Base-T.
10giga	Укажите, чтобы установить скорость 10 Гбит/с.
master | slave	Укажите статус порта: Master (основное устройство) или Slave (дополнительное устройство). Данный параметр применим только к устройствам, подключенным к порту 10GBase-T.
auto	Указывает, что для медных портов он определяет скорость и управление потоком через автосогласование с партнером по каналу. Указывает, что для оптоволоконных портов (1000BASE-SX/LX) включается опция автосогласования. Автосогласование начнет согласование тактовой частоты и управления потоком с партнером по каналу.
SPEED-LIST	(Опционально) Указывает список скоростей, с которыми коммутатор будет выполнять автосогласование. Скорость может быть **10**, **100** и/или **1000**. Используйте запятую (,) для разделения нескольких скоростей. Если список скоростей не указан, будут рекламироваться все скорости.

По умолчанию

Скорость будет установлена как **auto** для интерфейсов 1000BASE-T.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если указанная скорость не поддерживается аппаратно, будет отображено сообщение об ошибке. На устройстве с интерфейсом 100Base-FX всегда устанавливается фиксированная скорость 100 Мбит/с и режим полного дуплекса. Данный интерфейс не поддерживает функцию автосогласования. Изменить настройки данного интерфейса нельзя ни одной командой. На устройстве с интерфейсом 1000Base- SX/LX всегда устанавливается фиксированная скорость 1000 Мбит/с и режим полного дуплекса. Для данного интерфейса доступны только команды **speed 1000** и **speed auto**. Если на порту 1000Base-T установлена скорость

подключения 1000 Мбит/с, а на порту 10GBase-T – 10 Гбит/с, необходимо задать статус для данных портов: Master (основное устройство) или Slave (дополнительное устройство).

Чтобы включить функцию автосогласования, необходимо указать параметр **auto** или для скорости, или для режима дуплекса. При фиксированном режиме дуплекса и указании параметра **auto** для скорости будет согласована только скорость. Может быть установлена любая скорость в зависимости от выбранного режима дуплекса. При фиксированной скорости и указании параметра **auto** для режима дуплекса будет согласован только режим дуплекса.

При включенной функции автосогласования на порту 10GBase-R автоматически будет установлена скорость подключения в зависимости от типа SFP/SFP + (1000 Мбит/с или 10 Гбит/с).

Пример

В данном примере показано, как на интерфейсе Ethernet 1/0/1 включить автосогласование, при котором будут использоваться только скорости 10 Мбит/с или 100 Мбит/с.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# speed auto 10,100
Switch(config-if)#
```

73-5 speed auto-downgrade

Эта команда используется для включения автоматического понижения рекламируемой скорости в случае, если соединение не может быть установлено на доступной скорости. Для отключения этой команды используйте форму **no**.

speed auto-downgrade
no speed auto-downgrade

Параметры

Нет

По умолчанию

По умолчанию эта опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду для включения автоматического понижения рекламируемой скорости в случае, если соединение не может быть установлено на доступной скорости.

Пример

В этом примере показано, как включить автоматическое понижение скорости.

```
Switch#configure terminal
Switch(config)#interface eth1/0/5
Switch(config-if)#speed auto-downgrade
Switch(config-if)#
```

74. Команды управления системных файлов

74-1 boot config

Данная команда используется для указания конфигурационного файла, который будет использован при следующем запуске устройства.

boot config *URL*

Параметры

URL	Укажите URL конфигурационного файла, который будет использован при следующем запуске устройства.

По умолчанию

По умолчанию используется файл *config.cfg*.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

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 «switch-config.cfg», который будет использован при следующем запуске устройства.

```
Switch# configure terminal
Switch(config)# boot config c:/switch-config.cfg
Switch(config)#
```

74-2 boot image

Данная команда используется для указания файла образа, который будет использован при следующем запуске устройства.

boot image [check] [all] *URL*

Параметры

check	(Опционально) Укажите данный параметр для отображения информации о программном обеспечении для указанного

	файла (номер версии и описание модели).
all	(Опционально) Указывает на применение файла загрузочного образа ко всем коммутаторам в стеке.
URL	Укажите URL файла образа для загрузки.

По умолчанию

По умолчанию используется один файл образа для загрузки.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

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.

Образ резервного копирования определяется автоматически. Обычно ранее загруженный образ заменяется новым.

Пример

В данном примере показано, как указать файл под именем «switch-image1.had» в качестве файла образа для загрузки.

```
Switch# configure terminal
Switch(config)# boot image c:/switch-image1.had
Switch(config)#
```

В данном примере показано, как проверить указанный файл образа с именем «c:/runtime.switch.had». Информация о файле будет отображена после подтверждения его контрольной суммы.

```
Switch#configure terminal
Switch(config)#boot image check c:/runtime.wrongswitch.had

----------------------
Image information
----------------------
Version: 1.00.001
Description: D-Link Corporation TenGigabit Ethernet Switch

Switch(config)#
```

В данном примере показано, как проверить указанный файл образа с именем «runtime.wrongswitch.had». Контрольная сумма данного файла не прошла проверку, поэтому отобразилось сообщение об ошибке.

```
Switch# configure terminal
Switch(config)# boot image check runtime.wrongswitch.had
ERROR: Invalid firmware image.
Switch(config)#
```

В этом примере показано, как назначить образ следующей загрузки всем устройствам в режиме стекирования, если файл существует и действителен в устройстве 1, не существует в устройстве 2 и не действителен в устройстве 3.

```
Switch# configure terminal
Switch(config)# boot image all c:/switch-image1.had
ERROR: File not found on unit 2.
ERROR: Invalid firmware image on unit 3.
Switch(config)#
```

В этом примере показано, как проверить указанный файл образа с именем "c:/runtime.had" для всех устройств в режиме штабелирования. Контрольная сумма файла образа была проверена, и информация о файле образа отображается.

```
Switch# configure terminal
Switch(config)# boot image check all c:/runtime.had
----------------------
Image information of unit1
----------------------
Version    : 1.50.B018
Description: D-Link Gigabit Ethernet Switch

----------------------
Image information of unit2
----------------------
Version    : 1.50.B018
Description: D-Link Gigabit Ethernet Switch

----------------------
Image information of unit3
----------------------
Version    : 1.50.B018
Description: D-Link Gigabit Ethernet Switch
Switch (config)#
```

74-3 clear running-config

Данная команда используется для удаления текущей конфигурации системы (running configuration).

clear running-config

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

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 информация о стеке не удаляется, однако, 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#
```

74-4 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для удаления конфигурации системы, включая информацию о стеке. 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 all of system configuration as factory
default setting including IP parameters and stacking information.
Clear system configuration, save, reboot? (y/n) [n]  y

Saving configurations and logs to NV-RAM..... Done.
Please wait, the switch is rebooting...
```

74-5 configure replace

Данная команда используется для замены текущей конфигурации указанным конфигурационным файлом.

configure replace {{tftp: *//location/filename* **| flash:** *FILENAME***} [force]**

Параметры

tftp:	Укажите конфигурационный файл с TFTP-сервера.
//location/filename	Укажите URL конфигурационного файла на TFTP-сервере.
flash:	Укажите, что конфигурационный файл из NVRAM.
FILENAME	Укажите имя конфигурационного файла, хранящегося в NVRAM.
force	(Опционально) Укажите, чтобы принудительно применить команду без дополнительного подтверждения.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

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 данном примере показано, как заменить текущую конфигурацию файлом «config.cfg», хранящимся в NVRAM. Команда выполняется принудительно без дополнительного подтверждения.

```
Switch# configure replace flash: config.cfg force

 Executing script file config.cfg ......
 Executing done

Switch#
```

74-6 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 или сохранить его как файл в файловую систему. Укажите **attack-log** *UNIT-ID* в качестве URL источника, чтобы выгрузить журнал атак указанного Unit.
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 **bootconfig**. Укажите **flash: [***PATH-FILE-NAME***]** в качестве URL назначения, чтобы указать имя копируемого файла в файловой системе. При указании относительного пути файл будет загружен на все устройства в стеке и сохранен в текущем пути каждого Unit. При указании абсолютного пути файл будет загружен в место, которое было задано абсолютным путем. При отсутствии информации об Unit в абсолютном пути будет назначен основное устройство (Master).
LOCATION	Укажите IPv4-адрес TFTP/FTP/RCP-сервера или IPv6-адрес TFTP/FTP- сервера.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для копирования файлов в файловую систему, загрузки/выгрузки конфигурационного файла или файла образа, загрузки системного журнала на TFTP-сервер. Чтобы выгрузить текущую конфигурацию или сохранить ее в качестве загрузочной конфигурации, укажите **running-config** в качестве URL источника. Чтобы сохранить текущую конфигурация 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, используя метод 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 применить на коммутаторе конфигурацию как текущую, загруженную с TFTP-сервера, используя метод Increment. Имя конфигурационного файла: switch-config.cfg. TFTP- сервер: 10.1.1.254.

```
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 45421 bytes.
 Executing script file switch-config.cfg ......
 Executing done

Switch#
```

В данном примере 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://10.1.1.254/switch-config.cfg...
 Transmission start...
 Transmission finished, file length 45421 bytes.

Switch#
```

В данном 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#
```

В данном примере показано, как немедленно сохранить файл «switch-config.cfg» в NVRAM, используя метод Increment.

```
Switch# copy flash: switch-config.cfg running-config

Source filename [switch-config.cfg]?
Destination filename running-config? [y/n]:  y

 Executing script file switch-config.cfg ......
 Executing done

Switch#
```

В данном примере показано, как загрузить файл образа с TFTP-сервера на все устройства в стеке.

```
Switch# copy tftp: //10.1.1.254/image.had flash: image.had

Address of remote host [10.1.1.254]?
Source filename [image.had]?
Destination filename [image.had]?
 Accessing tftp://10.1.1.254/image.had...
 Transmission start...
 Transmission finished, file length 8315060 bytes.
 Transmission to slave start.................   Done.
 Transmission to slave finished, file length 8315060 bytes.
 Please wait, programming flash.............. Done.
 Wait slave programming flash complete...
 Done.

Switch#
```

В этом примере показано, как вывести сообщение об ошибке, если на флэш-памяти недостаточно места.

```
Switch# copy tftp: //10.1.1.254/image.had flash: image.had

Address of remote host [10.1.1.254]?
Source filename [image.had]?
Destination filename [image.had]?
 Accessing tftp://10.1.1.254/image.had...
 Transmission start...
 Transmission finished, file length 10293280 bytes.
 Transmission to slave start.................. Done.
 Transmission to slave finished, file length 10293280 bytes.
 Please wait, programming flash.............. 100 %
 Please wait, programming flash for language files .............Done.
 Wait slave programming flash complete...Fail.
 Unit 2: ERROR: Not enough space.

Switch#
```

74-7 ip tftp source-interface

Данная команда используется для указания интерфейса, IP-адрес которого будет использоваться в качестве адреса источника для инициирования TFTP-пакетов. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ip tftp source-interface *INTERFACE-ID*
no ip tftp source-interface

Параметры

INTERFACE-ID	Укажите IP-адрес интерфейса, который будет использоваться в качестве адреса источника для инициирования TFTP-пакетов.

По умолчанию

По умолчанию используется IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Эта команда используется для указания IP-адреса интерфейса, который будет использоваться в качестве адреса источника для инициирования пакетов TFTP. Чтобы использовать эту команду вместе с портом внеполосного управления, укажите идентификатор интерфейса для порта внеполосного управления.

Пример

В этом примере показано, как загрузить программное обеспечение с помощью интерфейса IP сети VLAN 100.

```
Switch# configure terminal
Switch(config)# ip tftp source-interface vlan100
Switch(config)#
```

74-8 show boot

Данная команда используется для отображения настроек конфигурационного файла и загрузочного образа.

show boot [unit *UNIT-ID***]**

Параметры

UNIT-ID	(Опционально) Укажите модуль (Unit), который необходимо отобразить.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Команда используется для отображения настроек конфигурационного файла и загрузочного образа.

Пример

В данном примере показано, как отобразить информацию о загрузке системы.

```
Switch#show boot

Unit 1
 Boot image: /c:/FW-1.70.005.had
 Boot config: /c:/config.cfg


Switch#
```

74-9 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) Указывает на отображение конфигураций команд, которые влияют на поведение коммутатора. Например, если STP была отключена, будет отображена только команда **disable stp**. Все остальные настройки нижнего уровня относительно STP отображаться не будут. Настройки нижнего уровня будут отображаться только в том случае, если настройки верхнего уровня включены. Если этот параметр не выбран, будут отображаться только измененные конфигурации, отличные от конфигурации по умолчанию.
all	(Опционально) Указывает на отображение всех конфигураций команд; включая команды, соответствующие параметрам по умолчанию. Если этот параметр не выбран, будут отображаться только измененные конфигурации, отличающиеся от конфигурации по умолчанию.
interface *INTERFACE-ID*	(Опционально) Указывает на отображение конфигураций команд, связанных с указанным интерфейсом. Введите здесь идентификатор интерфейса.
vlan *VLAN-ID*	(Опционально) Указывает на отображение конфигураций команд, соответствующих указанной VLAN.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Команда используется для отображения текущей конфигурации.

Пример

В данном примере показано, как отобразить содержимое текущего конфигурационного файла.

```
Switch#show running-config
Building configuration...

Current configuration : 1624 bytes

!-------------------------------------------------------------------------
!                DGS-1510-28XMP Gigabit Ethernet SmartPro Switch
!                                Configuration
!
!                            Firmware: Build 1.70.005
!           Copyright(C) 2020 D-Link Corporation. All rights reserved.
!-------------------------------------------------------------------------

line console
 session-timeout 0
!
line telnet
!
line ssh
!
ssh user admin authentication-method password
!
no ip domain lookup
ip name-server timeout 3
!
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

74-10 show startup-config

Данная команда используется для отображения содержимого конфигурационного загрузочного файла.

show startup-config

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Команда используется 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

!----------------------------------------------------------------------------
!                DGS-1510-28XMP Gigabit Ethernet SmartPro Switch
!                                Configuration
!
!                            Firmware: Build 1.70.005
!           Copyright(C) 2020 D-Link Corporation. All rights reserved.
!----------------------------------------------------------------------------

line console
!
line telnet
!
line ssh
!
ssh user admin authentication-method password
!
interface ethernet 1/0/1
!
interface ethernet 1/0/2
!
interface ethernet 1/0/3
!
interface ethernet 1/0/4
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

75. Команды System Log

75-1 clear logging

Данная команда используется для удаления сообщений логирования из буфера системного логирования.

clear logging

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда позволяет удалить все записи логирования из буфера системного логирования.

Пример

В данном примере показано, как удалить все записи логирования из буфера системного логирования.

```
Switch# clear logging

Clear logging? (y/n) [n] y

Switch#
```

75-2 logging buffered

Данная команда используется для включения логирования системных сообщений в локальный буфер сообщений. При использовании формы **no** команда отключит логирование системных сообщений в локальный буфер сообщений. Используйте команду **default logging buffered**, чтобы вернуть настройки 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 на этом уровне важности или более серьезном уровне будут логироваться в буфер сообщений. Значение может быть от 0 до 7, где 0 – наиболее важный уровень. Коды уровней важности: emergencies (чрезвычайные) – система не работоспособна (**0**), alerts (предупреждения) – система требует немедленного вмешательства (**1**), critical – состояние системы критическое (**2**), errors – сообщения об ошибках (**3**), warnings – предупреждения о возможных проблемах (**4**), notifications – уведомления о нормальных, но важных событиях (**5**), informational – информационные сообщения (**6**), debugging – отладочные сообщения (**7**). Если значение не указано, значение уровня по умолчанию – warnings (**4**).
SEVERITY-NAME	(Опционально) Укажите название уровня важности системных сообщений. Имена уровней важности: **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.
write-delay *SECONDS*	(Опционально) Укажите задержку периодической записи буфера логирования во FLASH-память на указанное количество секунд.

По умолчанию

По умолчанию используется уровень важности warning (4).

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Системные сообщения можно логировать в локальный буфер сообщений, локальную консоль или в другие места. Сообщения должны быть введены в локальный буфер сообщений перед отправкой в другие точки назначения.

Команда не будет применена, если указанный discriminator не существует. В таком случае будут применяться настройки по умолчанию.

Укажите уровень важности сообщений для ограничения системных сообщений, логируемых в буфер (это позволит уменьшить число логированных сообщений). Сообщения указанного уровня или выше будут логироваться в буфер. Если буфер будет заполнен, старые записи будут удалены, чтобы освободить место, необходимое для новых сообщений.

Содержимое буфера сообщений периодически будет сохраняться во FLASH-память, чтобы сообщения можно было восстановить при перезагрузке. Интервал сохранения записей из буфера во FLASH-память можно указать. Содержимое сообщений логирования во FLASH будет перезагружено в буфер логирования при перезагрузке.

Пример

В данном примере показано, как включить логирование сообщений в буфер логирования и ограничить логирование сообщений с уровнем важности errors или выше.

```
Switch# configure terminal
Switch(config)# logging buffered severity errors
Switch(config)#
```

75-3 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 на этом уровне важности или более серьезном уровне будут логироваться в буфер сообщений. Значение может быть от 0 до 7, где 0 – наиболее важный уровень. Коды уровней важности: emergencies (чрезвычайные) – система не работоспособна (**0**), alerts (предупреждения) – система требует немедленного вмешательства (**1**), critical – состояние системы критическое (**2**), errors – сообщения об ошибках (**3**), warnings – предупреждения о возможных проблемах (**4**), notifications – уведомления о нормальных, но важных событиях (**5**), informational – информационные сообщения (**6**), debugging – отладочные сообщения (**7**). Если значение не указано, значение уровня по умолчанию – warnings (**4**).
SEVERITY-NAME	(Опционально) Укажите название уровня важности системных сообщений. Имена уровней важности: **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

Уровень команды по умолчанию

Уровень 12

Использование команды

Системные сообщения можно логировать в локальный буфер сообщений, локальную консоль или другие точки назначения. Сообщения должны быть введены в локальный буфер сообщений перед отправкой в консоль.

Команда не будет применена, если указанный discriminator не существует. В таком 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)#
```

75-4 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 discriminator *NAME*

Параметры

NAME	Укажите имя discriminator.
facility	(Опционально) Укажите подфильтр согласно настройке facility.
STRING	Укажите одно или более имен facility. Если используется несколько имен, они должны быть разделены запятой, без пробелов до и после запятой.
includes	Укажите для включения совпадающих сообщений. Несовпадающие сообщения будут фильтроваться.
drops	Укажите для фильтрации совпадающих сообщений.
severity	(Опционально) Укажите подфильтр 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Настройка существующего параметра discriminator. При вводе команды более ранние настройки будут переписаны на новые. 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)#
```

75-5 logging monitor

Эта команда используется для включения протоколирования системных сообщений на терминалах, таких как Telnet и SSH. Для отключения функции используйте форму **no** этой команды.

logging monitor [severity {*SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [discriminator** *NAME***]**
no logging monitor

Параметры

SEVERITY-LEVEL	(Опционально) Укажите уровень важности системных сообщений. Сообщения на этом уровне важности или более серьезном уровне будут логироваться в буфер сообщений. Значение может быть от 0 до 7, где 0 – наиболее важный уровень. Коды уровней важности: emergencies (чрезвычайные) – система не работоспособна (**0**), alerts (предупреждения) – система требует немедленного вмешательства (**1**), critical – состояние системы критическое (**2**), errors – сообщения об ошибках (**3**), warnings – предупреждения о возможных проблемах (**4**), notifications – уведомления о нормальных, но важных событиях (**5**), informational – информационные сообщения (**6**), debugging – отладочные сообщения (**7**). Если значение не указано, значение уровня по умолчанию – warnings (**4**).
SEVERITY-NAME	(Опционально) Укажите название уровня важности системных сообщений. Имена уровней важности: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).
discriminator	(Опционально) Указывает фильтровать сообщение для отправки на терминалы, такие как Telnet или SSH, на основе **discriminator**.

По умолчанию

По умолчанию эта опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Системные сообщения могут быть зарегистрированы в локальном буфере сообщений или в других местах назначения. Сообщения должны сначала попасть в локальный буфер сообщений, прежде чем они могут быть отправлены в другие пункты назначения.

Эта команда не действует, если указанный дискриминатор не существует. Таким образом, применяется настройка команды по умолчанию.

Укажите уровень серьезности сообщений, чтобы ограничить системные сообщения, которые регистрируются на терминале. На терминал будут записываться сообщения с указанным уровнем серьезности или выше.

Пример

В этом примере показано, как включить регистрацию сообщений на терминале и ограничить регистрацию сообщений с уровнем безопасности ошибки или выше.

```
Switch#configure terminal
Switch(config)#logging monitor severity errors
Switch(config)#
```

75-6 logging server

Данная команда используется для создания серверного узла SYSLOG для логирования системных сообщений или вывода при отладке. При использовании формы **no** команда удалит серверный узел SYSLOG.

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 серверного узла SYSLOG.
IPV6-ADDRESS	Укажите IPv6-адрес серверного узла логирования.
SEVERITY-LEVEL	(Опционально) Укажите уровень важности системных сообщений. Сообщения на этом уровне важности или более серьезном уровне будут логироваться в буфер сообщений. Значение может быть от 0 до 7, где 0 – наиболее важный уровень. Коды уровней важности: emergencies (чрезвычайные) – система не работоспособна

	(**0**), alerts (предупреждения) – система требует немедленного вмешательства (**1**), critical – состояние системы критическое (**2**), errors – сообщения об ошибках (**3**), warnings – предупреждения о возможных проблемах (**4**), notifications – уведомления о нормальных, но важных событиях (**5**), informational – информационные сообщения (**6**), debugging – отладочные сообщения (**7**). Если значение не указано, значение уровня по умолчанию – warnings (**4**).
SEVERITY-NAME	(Опционально) Укажите название уровня важности системных сообщений. Имена уровней важности: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).
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 для 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Системные сообщения можно логировать в локальный буфер сообщений, локальную консоль или на удаленные узлы. Сообщения должны быть введены в локальный буфер сообщений перед отправкой на сервер логирования.

Ниже представлена таблица значений Facility.

Номер Facility	Имя Facility	Описание
0	kern	Сообщения ядра
1	user	Сообщения уровня пользователя

2	mail	Система почты
3	daemon	Системные daemon
4	auth1	Сообщения системы безопасности/авторизации
5	syslog	Сообщения, генерируемые SYSLOG
6	lpr	Подсистема Line Printer
7	news	Подсистема сетевых новостей
8	uucp	Подсистема UUCP
9	clock1	Clock daemon
10	auth2	Сообщения системы безопасности/авторизации
11	ftp	FTP daemon
12	ntp	Подсистема NTP
13	logaudit	Аудит логирования
14	logalert	Предупреждение логирования
15	clock2	Clock daemon (note 2)
16	local0	Локальное использование 0 (local0)
17	local1	Локальное использование 1 (local1)
18	local2	Локальное использование 2 (local2)
19	local3	Локальное использование 3 (local3)
20	local4	Локальное использование 4 (local4)
21	local5	Локальное использование 5 (local5)
22	local6	Локальное использование 6 (local6)
23	local7	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)#
```

75-7 logging source-interface

Данная команда используется для указания IP-адреса интерфейса, который будет использоваться в качестве адреса источника для отправки пакетов SYSLOG. При использовании формы **no** команда вернется к настройкам по умолчанию.

logging source-interface *INTERFACE-ID*
no logging source-interface

Параметры

INTERFACE-ID	Укажите IP-адрес интерфейса, который будет использоваться в качестве адреса источника для отправки пакетов SYSLOG.

По умолчанию

По умолчанию используется IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для указания IP-адреса интерфейса, который будет использоваться в качестве адреса источника для отправки пакетов SYSLOG.

Пример

В данном примере показано, как настроить VLAN 100 в качестве интерфейса источника для пакетов SYSLOG.

```
Switch# configure terminal
Switch(config)# logging source-interface vlan 100
Switch(config)#
```

75-8 show logging

Данная команда используется для просмотра системных сообщений, логированных в локальном буфере.

show logging [all | [*REF-SEQ*] [+ *NN* | - *NN*]]

Параметры

all	(Опционально) Укажите для отображения всех записей лога, начиная с последних.
REF-SEQ	(Опционально) Укажите для отображения с номера, следующего за указанным.
+ *NN*	(Опционально) Укажите количество сообщений, появившихся после указанного номера, следующим за указанным. Если значение не указано, отображение начинается от самых давних сообщений в буфере.
- *NN*	(Опционально) Укажите количество сообщений, появившихся до указанного номера, следующим за указанным. Если значение не указано, отображение начинается от самых последних сообщений в буфере.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Команда используется для просмотра системных сообщений, логированных в локальном буфере.

Каждое логированное в буфер сообщение ассоциировано с номером последовательности. При логировании сообщения назначается номер последовательности, начиная с 1. Номер последовательности вернется к 1 после достижения 100000.

Если пользователь указывает отображение количества сообщений после номера, следующим за указанным, более поздние сообщения будут отображаться до новых. Если пользователь указывает отображение количества сообщений с номера, следующим за указанным, новые сообщения будут отображаться до более поздних.

Если команда введена без опций, будет отображено 200 записей, начиная от самых последних.

Пример

В данном примере показано, как отобразить сообщения в локальном буфере сообщений.

```
Switch# show Switch# show logging

Total number of buffered messages: 2
#2 2015-03-25 16:37:36 Unit 1, Successful login through Console (Username: Anonymous)
#1 2015-03-25 16:35:54 INFO(6) Port eth1/0/1 link up, 1000Mbps FULL duplex

Switch#
```

75-9 show attack-logging

Данная команда используется для просмотра логированных сообщений об атаках.

show attack-logging unit *UNIT-ID* **[index** *INDEX***]**

Параметры

UNIT-ID	Укажите модуль (Unit), для которого необходимо отобразить логированные сообщения об атаке.
index *INDEX*	Укажите список номеров index-записей, которые необходимо отобразить. Если значение не указано, отображаться будут все данные из журнала атак.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для просмотра логированных сообщений журнала об атаках. Такие сообщения относятся к сообщениям журнала, управляемым такими модулями, как DOS и port-security. Данный тип логированных сообщений может генерировать большое число сообщений, из-за чего в системе быстро закончится память для логирования. Поэтому для данного типа сообщений в системном журнале хранится только первое логирование, генерируемое каждую минуту, а остальные хранятся в отдельной таблице с именем attack log (журнал атак).

Пример

В данном примере показано, как отобразить первое логированное сообщение об атаке.

```
Switch# show attack-logging index 1
Attack log messages:
1  2015-03-24 15:00:14 CRIT(2) Land attack is blocked from (IP: 10.72.24.1 Port: 7)
Switch#
```

75-10 clear attack-logging

Данная команда используется для удаления сообщений об атаках.

clear attack-logging {unit *UNIT-ID* **| all}**

Параметры

unit *UNIT-ID*	Укажите модуль (Unit), для которого необходимо удалить логированные сообщения об атаке.
all	Укажите для удаления всех записей.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

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#
```

---

76. Команды времени и SNTP

76-1 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 (January, Jan, February, Feb и т. д.).
YEAR	Укажите текущий год без сокращений.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

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 этом примере показано, как вручную установить программные часы на 6:00 вечера 4 июля 2014 года.

```
Switch# clock set 18:00:00 4 jul 2014
Switch#
```

76-2 clock summer-time

Данная команда используется для настройки автоматического перехода на летнее время. Используйте форму **no**, чтобы отключить автоматический переход на летнее время.

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 порядковый номер месяца в диапазоне от 1 до 12, где 1 – это январь, 2 – февраль 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. Доступный диапазон смещения – 30, 60, 90 и 120 минут.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 этом примере показано, как указать, что летнее время начинается в первое воскресенье июня в 2 часа ночи и заканчивается в последнее воскресенье октября в 2 часа ночи.

```
Switch# configure terminal
Switch(config)# clock summer-time recurring 1 sun jun 2:00 last sun oct 2:00
Switch(config)#
```

76-3 clock timezone

Данная команда используется для настройки и отображения часового пояса. Используйте форму **no**, чтобы настроить время в формате UTC (всемирное координированное время).

clock timezone {+ | -} *HOURS-OFFSET* **[***MINUTES-OFFSET***]**
no clock timezone

Параметры

+	Укажите количество часов, которых необходимо прибавить к UTC.
-	Укажите количество часов, которых 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

Уровень команды по умолчанию

Уровень 12

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)#
```

76-4 show clock

Данная команда используется для отображения информации о времени и дате.

show clock

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Также данная команда используется 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, 2000-01-30
     Time Zone              : UTC +00:00
     Daylight Saving Time   : Disabled

Switch#
```

76-5 show sntp

Данная команда используется для отображения информации о сервере SNTP.

show sntp

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется 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
---------------------------------------------- ------- ---------------
10.0.0.11                                      4       00:02:02
10::2                                          ------- ---------------
FE80::1111%vlan1                               ------- ---------------
---------------------------------------------- ------- ---------------

Total Entries:3

Switch#
```

76-6 sntp server

Данная команда используется для синхронизации системного времени с сервером SNTP. Используйте форму **no**, чтобы удалить сервер из списка серверов SNTP.

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

Уровень команды по умолчанию

Уровень 12

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 предоставляет сложные механизмы фильтрации и статистической обработки. Кроме того, SNTP не проверяет подлинность трафика, хотя с помощью настройки расширенного списка доступа можно обеспечить определённую степень защиты.

Введите данную команду один раз для каждого сервера NTP. Настроить систему и включить SNTP можно также с помощью команды **sntp broadcast client global configuration**. 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)#
```

76-7 sntp enable

Данная команда используется для включения функции SNTP. Используйте форму **no**, чтобы отключить функцию SNTP.

sntp enable
no sntp enable

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения/отключения функции SNTP.

Пример

В данном примере показано, как включить функцию SNTP.

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

76-8 sntp interval

Данная команда используется для настройки интервала синхронизации часов SNTP-клиента с сервером. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки интервала опроса (Polling Interval).

Пример

В данном примере показано, как настроить интервал на 100 секунд.

```
Switch# configure terminal
Switch(config)# sntp interval 100
Switch(config)#
```

77. Команды временного диапазона

77-1 periodic

Данная команда используется в режиме Time-Range Configuration Mode для указания профиля диапазона времени. Используйте форму **no**, чтобы удалить указанный временной диапазон.

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:*	Укажите день недели (monday, tuesday, wednesday, thursday, friday, satur- day, 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

Уровень команды по умолчанию

Уровень 12

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)#
```

77-2 show time-range

Данная команда используется для отображения конфигурации профиля диапазона времени.

show time-range [*NAME*]

Параметры

NAME	(Опционально) Укажите имя профиля диапазона времени, который необходимо отобразить.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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#
```

77-3 time-range

Данная команда используется для указания профиля диапазона времени и входа в режим Time-Range Configuration Mode. Используйте форму **no**, чтобы удалить временной диапазон.

time-range *NAME*
no time-range *NAME*

Параметры

NAME	Укажите имя профиля диапазона времени, который необходимо настроить. Максимально допустимое количество символов – 32.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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, и отобразить его с помощью команды **show time-range** не получится.

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)#
```

78. Команды Traffic Segmentation

78-1 show traffic-segmentation forward

Данная команда используется для отображения конфигурации Traffic Segmentation на указанных или всех портах.

show traffic-segmentation forward [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально) Укажите интерфейсы, которые необходимо отобразить. Допустимый интерфейс: 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

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

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#
```

78-2 traffic-segmentation forward

Данная команда используется для ограничения продвижения пакетов в L2 домене, приходящих на настроенный порт. Используйте форму **no**, чтобы удалить ограничения продвижения пакетов в L2 домене.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

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 использовать 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 Ethernet-порта 1/0/1. Установленное ограничение: от Ethernet-порта 1/0/3 до Ethernet- порта 1/0/6.

```
Switch# configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#traffic-segmentation forward interface ethernet 1/0/3-6
Switch(config-if)#
```

79. Команды безопасности транспортного уровня (TLS)

79-1 no certificate

Эта команда используется для удаления импортированного сертификата.

no certificate *NAME*

Параметры

NAME	Укажите имя удаляемого сертификата.

По умолчанию

Нет

Режим ввода команды

Certificate Chain Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте команду **show crypto pki trustpoints**, чтобы получить список имен импортированных сертификатов. Затем используйте эту команду для удаления импортированных сертификатов точки доверия. Если указанный сертификат является локальным сертификатом, соответствующий закрытый ключ будет удален одновременно. При удалении закрытого ключа будет выведено предупреждение.

Пример

В этом примере показано, как удалить импортированный сертификат с именем *tongken.ca* из точки доверия *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)#
```

79-2 crypto pki import pem

Эта команда используется для импорта сертификата CA или сертификата и ключей коммутатора в точку доверия 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 точки доверия, связанной с импортированными сертификатами и парами ключей.
FILE-SYSTEM	Укажите файловую систему для сертификатов и пар ключей. После указанной файловой системы требуется двоеточие (:). Например, **flash**: представляет систему FLASH.
DIRECTORY	(Опционально) Укажите имя каталога, в который коммутатор должен импортировать сертификаты и пары ключей на коммутаторе или TFTP-сервере.
FILE-NAME	Указывает имя импортируемых сертификатов и пар ключей. По умолчанию коммутатор будет добавлять это имя с *.ca*, *.prv* и *.crt* для сертификата ЦС, закрытого ключа и сертификата соответственно.
password *PASSWORD-PHRASE*	(Опционально) Указывает зашифрованную фразу пароля, которая используется для отмены шифрования при импорте закрытых ключей. Фраза пароля представляет собой строку длиной до 64 символов. Если фраза пароля не указана, будет использована строка NULL.
tftp:	Указывает URL-адрес источника для сетевого сервера TFTP.
IP-ADDRESS	Укажите IP-адрес сервера TFTP.
ca	Укажите, чтобы импортировать только сертификат ЦС.
local	Указывает импортировать только локальные пары сертификатов и ключей.

both	Указывает на импорт сертификата ЦС, локального сертификата и пар ключей.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Эта команда позволяет администраторам импортировать сертификаты и пары ключей в файлах формата PEM.

Соответствующие сертификаты и пары ключей должны быть импортированы 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. Клиент SSL, имеющий только сертификат и ключ RSA, не может установить соединение с сервером SSL, имеющим только сертификат и ключ DSA.

Импортированный(ые) сертификат(ы) может(ут) образовывать цепочку сертификатов, которая устанавливает последовательность доверенных сертификатов от сертификата сверстника до сертификата корневого ЦС. ЦС точки доверия - это центр сертификации, настроенный на коммутаторе как доверенный ЦС. Любой полученный сертификат сверстника будет принят, если он подписан локальным доверенным ЦС или его подчиненными.

Если указанная точка доверия не существует, будет выдано сообщение об ошибке.

Пример

В этом примере показано, как импортировать сертификаты (CA и локальные) и файлы пар ключей в точку доверия "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)#
```

79-3 crypto pki trustpoint

Эта команда используется для объявления точки доверия, которую будет использовать коммутатор. Используйте форму **no** этой команды для удаления всех сертификатов и пар ключей, связанных с точкой доверия.

crypto pki trustpoint *NAME*
no crypto pki trustpoint *NAME*

Параметры

NAME	Укажите, чтобы создать имя для точки доверия.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте эту команду для объявления точки доверия, которая может быть самоподписанным корневым центром сертификации (ЦС) или подчиненным ЦС. При вводе этой команды вы войдете в режим конфигурации CA-Trust-Point.

Пример

В этом примере показано, как объявить доверительную точку "TP1" и указать ее как основную доверительную точку.

```
Switch# configure terminal
Switch(config)# crypto pki trustpoint TP1
Switch(ca-trustpoint)# primary
Switch(ca-trustpoint)#
```

79-4 crypto pki certificate chain

Эта команда используется для входа в режим конфигурации цепочки сертификатов.

crypto pki certificate chain *NAME*

Параметры

NAME	Укажите имя для точки доверия.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте эту команду для входа в режим конфигурации цепочки сертификатов. Если указанное имя точки доверия не существует, будет выведено сообщение об ошибке.

Пример

В этом примере показано, как войти в режим конфигурации цепочки сертификатов.

```
Switch# configure terminal
Switch(config)# crypto pki certificate chain TP1
Switch(config-cert-chain)#
```

79-5 crypto pki certificate generate

Эта команда используется для генерации 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

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте эту команду для генерации нового self-signed сертификата независимо от наличия или отсутствия встроенного self-signed сертификата. Коммутатор создаст новый самоподписанный сертификат автоматически, если после загрузки коммутатора сертификат не был обнаружен.

Сертификат, созданный этой командой, не влияет на загруженные пользователем сертификаты.

Примечание: Эта команда поддерживает только self-signature сертификат RSA с длиной ключа 2048.

Пример

В этом примере показано, как сгенерировать новый self-signed certificate.

```
Switch# configure terminal
Switch(config)# crypto pki certificate generate

Start generating key ...
Start generating self-signed certificate ...
Done.
Switch(config)#
```

79-6 primary

Эта команда используется для назначения указанной доверительной точки в качестве основной доверительной точки коммутатора. Используйте форму **no** этой команды, чтобы снять привязку настройки.

primary
no primary

Параметры

Нет

По умолчанию

По умолчанию эта функция отключена.

Режим ввода команды

CA-Trust-Point Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте команду primary для указания данной точки доверия в качестве основной. Эта точка доверия может быть использована в качестве точки доверия по умолчанию, когда приложение явно не указывает, какая точка доверия центра сертификации (ЦС) должна быть использована. Только одна точка доверия может быть указана в качестве основной. Последняя точка доверия, указанная в качестве основной, перезаписывает предыдущую.

Пример

В этом примере показано, как настроить точку доверия "TP1" в качестве основной точки доверия.

```
Switch# configure terminal
Switch(config)# crypto pki trustpoint TP1
Switch(ca-trustpoint)# primary
Switch(ca-trustpoint)#
```

79-7 show crypto pki trustpoints

Эта команда используется для отображения точек доверия, настроенных в коммутаторе.

show crypto pki trustpoints [*TRUSTPOINT***]**

Параметры

TRUSTPOINT	(Опционально) Укажите имя точки доверия, которая будет отображаться.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если параметр не указан, будут отображены все точки доверия.

Пример

В этом примере показано, как отобразить все точки доверия.

```
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#
```

79-8 show ssl-service-policy

Эта команда используется для отображения политики службы SSL.

show ssl-service-policy [*POLICY-NAME***]**

Параметры

POLICY-NAME	(Опционально) Указывает имя политики службы SSL.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если имя политики службы SSL не указано, будут отображены все политики службы SSL.

Пример

В этом примере показано, как отобразить все политики служб SSL.

```
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#
```

79-9 ssl-service-policy

Эта команда используется для настройки политики службы SSL. Используйте форму **no** этой команды, чтобы удаления политики обслуживания SSL.

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	Указывает имя политики службы SSL.
version *VERSION*	(Опционально) Указывает версию TLS. Можно использовать одно из следующих ключевых слов: **tls1.0** - Указывает на использование TLS версии 1.0 в качестве политики службы SSL. **tls1.1** - Указывает на использование TLS версии 1.1 в качестве политики службы SSL. **tls1.2** - Указывает на использование TLS версии 1.2 в качестве политики службы SSL.
ciphersuite *CIPHERSUITE*	(Опционально) Указывает наборы шифров, которые должны использоваться службой безопасности при согласовании соединения с удаленным аналогом. Если набор шифров не настроен, клиент и сервер SSL будут согласовывать лучший набор шифров, который они оба поддерживают, из списка доступных наборов шифров. Можно указать несколько наборов шифров, которые будут использоваться. Используйте форму no этой команды, чтобы отключить выбранные наборы шифров. Можно использовать следующие ключевые слова: **dhe-dss-3des-ede-cbc-sha** - Указывает на использование обмена ключами DH с шифрованием 3DES-EDE-CBC и SHA для дайджеста сообщений. **rsa-3des-ede-cbc-sha** - Указывает на использование обмена ключами RSA с 3DES и DES-EDE3-CBC для шифрования сообщений и алгоритма безопасного хэширования (SHA) для дайджеста сообщений. **rsa-rc4-128-sha** - указывает на использование обмена ключами RSA со 128-битным шифрованием RC4 для шифрования сообщений и SHA для дайджеста сообщений. **rsa-rc4-128-md5** - указывает на использование обмена ключами RSA со 128-битным шифрованием RC4 для шифрования сообщений и Message Digest 5 (MD5) для дайджеста сообщений. **rsa-export-rc4-40-md5** - Указывает на использование обмена ключами RSA EXPORT с RC4 40 бит для шифрования сообщений и MD5 для дайджеста сообщений. **rsa-aes-128-cbc-sha** - Указывает на использование обмена ключами RSA со 128-битным шифрованием AES для шифрования сообщений и SHA для дайджеста сообщений. **rsa-aes-256-cbc-sha** - Указывает на использование обмена ключами RSA с 256-битным шифрованием AES для шифрования сообщений и SHA для дайджеста сообщений. **rsa-aes-128-cbc-sha256** - Указывает на использование обмена ключами RSA со 128-битным шифрованием AES для шифрования сообщений и SHA 256-бит для дайджеста сообщений. **rsa-aes-256-cbc-sha256** - Указывает на использование обмена ключами RSA с 256-битным шифрованием AES для шифрования сообщений и SHA 256-bit для дайджеста сообщений.

	dhe-dss-aes-256-cbc-sha - Указывает на использование обмена ключами DH с 256-битным шифрованием AES и SHA для дайджеста сообщений. **dhe-rsa-aes-256-cbc-sha** - Указывает на использование обмена ключами DH с 256-битным шифрованием AES и SHA для дайджеста сообщений.
secure- trustpoint *TRUSTPOINT*	(Опционально) Указывает имя доверительной точки, которая должна использоваться в SSL handshake. Если этот параметр не указан, будет использоваться точка доверия, указанная в качестве основной. Если основная точка доверия не указана, будут использоваться встроенные пары сертификат/ключ. В форме **no** этой команды указанная точка доверия будет отменена, а затем будут использоваться встроенные пары сертификат/ключ.
session-cache-timeout *TIME-OUT*	(Опционально) Указывает значение тайм-аута в секундах для информации, хранящейся в кэше сеансов SSL. Допустимый диапазон - от 60 до 86400. Если этот параметр не настроен, тайм-аут кэша сеанса по умолчанию составляет 600 секунд. В форме no этой команды тайм-аут кэша SSL-сессии будет возвращен к значению по умолчанию.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Эта команда используется для настройки политики службы SSL.

Пример

В этом примере показано, как настроить политику службы SSL "ssl-server", которая связывает точку доверия "TP1".

```
Switch# configure terminal
Switch(config)# ssl-service-policy ssl-server secure-trustpoint TP1
Switch(config)#
```

80. Команды Virtual LAN (VLAN)

80-1 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки допустимых типов кадров на порту.

Пример

В данном примере показано, как настроить допустимый тип кадров tagged-only для порта Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# acceptable-frame tagged-only
Switch(config-if)#
```

80-2 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для включения проверки входящих кадров, получаемых интерфейсом. При включенной проверке пакет будет отброшен в том случае, если принимающий порт не является членом VLAN, классифицированной для получаемого пакета.

Пример

В данном примере показано, как настроить проверку входящего трафика для включенного порта Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ingress-checking
Switch(config-if)#
```

80-3 show-vlan

Данная команда используется для отображения параметров для всех настроенных VLAN или одной VLAN на коммутаторе.

show vlan [*VLAN-ID* **[, | -] | interface [***INTERFACE-ID* **[, | -]] | mac-vlan]**

Параметры

VLAN-ID	(Опционально) Список VLAN для отображения информации о портах- участниках. Если VLAN не указана, то отображаются все VLAN. Корректный диапазон: от 1 до 4094.
,	(Опционально) Диапазон VLAN или разделение VLAN от предыдущего диапазона. Перед и после запятой использование пробела недопустимо.
-	(Опционально) Диапазон VLAN. Перед дефисом и после дефиса использование пробела недопустимо.
interface *INTERFACE-ID*	(Опционально) Порт для отображения настроек, касающихся VLAN.
,	(Опционально) Диапазон интерфейсов или разделение интерфейсов от предыдущего диапазона. Перед и после

	запятой использование пробела недопустимо.
-	(Опционально) Диапазон интерфейсов. Перед дефисом и после дефиса использование пробела недопустимо.
mac-vlan	(Опционально) Указывается для отображения информации о VLAN на основе MAC-адресов.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения параметров для всех настроенных VLAN или одной VLAN на коммутаторе.

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 ethernet 1/0/1-1/0/4.

```
Switch#show vlan interface eth1/0/1-1/0/4

 eth1/0/1
   VLAN mode              : Hybrid
   Native VLAN            : 1
   Hybrid untagged VLAN   : 1
   Hybrid tagged VLAN     :
   Ingress checking       : Enabled
   Acceptable frame type  : Admit-All
   Dynamic tagged VLAN    :

 eth1/0/2
   VLAN mode              : Hybrid
   Native VLAN            : 1
   Hybrid untagged VLAN   : 1
   Hybrid tagged VLAN     :
   Ingress checking       : Enabled
   Acceptable frame type  : Admit-All
   Dynamic tagged VLAN    :

 eth1/0/3
   VLAN mode              : Hybrid
   Native VLAN            : 1
   Hybrid untagged VLAN   : 1
   Hybrid tagged VLAN     :
   Ingress checking       : Enabled
   Acceptable frame type  : Admit-All
   Dynamic tagged VLAN    :

 eth1/0/4
   VLAN mode              : Hybrid
   Native VLAN            : 1
   Hybrid untagged VLAN   : 1
   Hybrid tagged VLAN     :
   Ingress checking       : Enabled
   Acceptable frame type  : Admit-All
   Dynamic tagged VLAN    :

Switch#
```

80-4 switchport access vlan

Данная команда используется для указания 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	Access VLAN интерфейса.

По умолчанию

По умолчанию access VLAN является VLAN 1.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда вступает в силу, когда интерфейс настроен в режиме доступа (access mode) или режиме dot1q-tunnel mode. VLAN, указанная в качестве access VLAN, не должна обязательно существовать для настройки команды. Может быть указана только одна access VLAN. Следующая команда перезаписывает предыдущую команду.

Пример

В данном примере показано, как настроить ethernet 1/0/1 в режиме доступа (access mode) с access VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1000
Switch(config-if)#
```

80-5 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) Порт, который будет добавлен в указанную(-ые) VLAN.
tagged	Указывает порт в качестве тегированного для указанной(-ых) VLAN.

untagged	Указывает порт в качестве нетегированного для указанной(-ых) VLAN.
remove	Порт, который будет удален из указанной(-ых) VLAN.
VLAN-ID	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) Диапазон VLAN или разделение VLAN от предыдущего диапазона. Перед и после запятой использование пробела недопустимо.
-	(Опционально) Диапазон VLAN. Перед дефисом и после дефиса использование пробела недопустимо.

По умолчанию

По умолчанию гибридный порт является нетегированным членом VLAN 1.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Настраивая команду hybrid VLAN несколько раз с разными VLAN ID порт может стать тегированным или нетегированным членом нескольких VLAN.
Когда разрешенная VLAN указана только как VLAN ID, следующая команда перезапишет предыдущую команду. Если новый нетегированный разрешенный список VLAN перекрывается с текущим списком тегированных разрешенных VLAN, то перекрывающаяся часть будет изменена на нетегированную разрешенную VLAN. С другой стороны, если новый список тегированных разрешенных VLAN перекрывается с текущим списком нетегированных разрешенных VLAN, то перекрывающаяся часть будет изменена на тегированную разрешенную VLAN. Последняя команда вступит в силу. VLAN не должна обязательно существовать для настройки команды.

Пример

В данном примере показано, как настроить ethernet 1/0/1 в качестве тегированного порта VLAN 1000 и нетегированного порта VLAN 2000 и 3000.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
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)#
```

80-6 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

Уровень команды по умолчанию

Уровень 12

Использование команды

При настройке привязки гибридного порта к его native VLAN используйте команду **switchport hybrid allowed vlan**, чтобы добавить native VLAN в ее разрешенную VLAN. Указанная VLAN не должна обязательно существовать для применения этой команды. Команда вступает в силу, когда интерфейс настроен в гибридном режиме.

Пример

В данном примере показано, как настроить ethernet 1/0/1, чтобы он стал гибридным интерфейсом, и настроить PVID 20.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
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)#
```

80-7 switchport mode

Данная команда используется для указания режима VLAN (VLAN mode) для порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

switchport mode {access | hybrid | trunk}
no switchport mode

Параметры

access	Указывает порт в качестве порта доступа.
hybrid	Указывает порт в качестве гибридного порта.
trunk	Указывает порт в качестве trunk-порта.

По умолчанию

По умолчанию установлена опция **hybrid**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Когда порт установлен в режим доступа (access mode), этот порт будет нетегированным членом access VLAN, настроенной для порта. Когда порт установлен в гибридный режим (hybrid mode), порт может быть нетегированным или тегированным членом всех настроенных VLAN. Цель этого режима VLAN - поддержка protocol VLAN, VLAN на основе подсетей (subnet-based VLAN) и VLAN на основе MAC-адресов (MAC-based VLAN).

Когда порт настроен в режим trunk, этот порт является либо тегированным, либо нетегированным членом его native VLAN и может быть тегированным членом других настроенных VLAN. Цель trunk- порта - поддержка соединения switch-to-switch. Когда порт установлен в режим dot1q-tunnnel mode, порт действует как порт UNI в service VLAN.

При изменении режима switch-port mode настройки, связанные с VLAN и ассоциированные с предыдущим режимом, будут утеряны.

Пример

В данном примере показано, как настроить ethernet 1/0/1 в качестве trunk-порта.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)#
```

80-8 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	VLAN, которые разрешены на интерфейсе.
add	Добавление списка указанных VLAN в список разрешенных VLAN.
remove	Удаление списка указанных VLAN из списка разрешенных VLAN.

except	Указывает, что разрешены все VLAN, за исключением VLAN, находящихся в списке исключений.
VLAN-ID	Список разрешенных VLAN или список VLAN, которые должны быть добавлены в список разрешенных VLAN или удалены из него.
,	(Опционально) Диапазон VLAN или разделение VLAN от предыдущего диапазона. Перед и после запятой использование пробела недопустимо.
-	(Опционально) Диапазон VLAN. Перед дефисом и после дефиса использование пробела недопустимо.

По умолчанию

По умолчанию все VLAN разрешены.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда вступает в силу, только когда интерфейс настроен в режиме trunk mode. Если VLAN разрешена на trunk-порту, то порт станет тегированным членом 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 ethernet 1/0/1 в качестве тегированного члена VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 1000
Switch(config-if)#
```

80-9 switchport trunk native vlan

Данная команда используется для указания native VLAN ID интерфейса в режиме trunk mode. 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда вступает в силу, только когда интерфейс настроен в режиме trunk mode. Когда 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. Когда 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 ethernet 1/0/1 в качестве интерфейса trunk и native VLAN 20.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 20
Switch(config-if)#
```

80-10 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) Диапазон VLAN или разделение VLAN от предыдущего диапазона. Перед и после запятой использование пробела недопустимо.
-	(Опционально) Диапазон VLAN. Перед дефисом и после дефиса использование пробела недопустимо.

По умолчанию

VLAN ID 1 существует в системе в качестве VLAN по умолчанию.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду глобальной настройки **vlan** для создания VLAN. Ввод команды **vlan** с VLAN ID влечет 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 до1005.

```
Switch# configure terminal
Switch(config)# vlan 1000-1005
Switch(config-vlan)#
```

80-11 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 (включая начальные нули), которые равны VLAN ID.

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для указания имени VLAN. Имя VLAN должно быть уникальным в административном домене.

Пример

В данном примере показано, как настроить имя VLAN «admin-vlan» для VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# name admin-vlan
Switch(config-vlan)#
```

80-12 mac-vlan

Данная команда используется для создания привязки VLAN на основе MAC-адреса. Используйте форму **no** для удаления привязки VLAN на основе MAC-адреса.

mac-vlan *MAC-ADDRESS* **vlan** *VLAN-ID* **[priority** *COS-VALUE***]**
no mac-vlan *MAC-ADDRESS*

Параметры

MAC-ADDRESS	MAC-адрес для привязки.
vlan *VLAN-ID*	VLAN ID для привязки VLAN на основе MAC-адреса.
priority *COS-VALUE*	(Опционально) Значение приоритета CoS. Если параметр не указан, то значением CoS по умолчанию является 0.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для создания привязки VLAN на основе MAC-адреса. Классификация привязки будет применена к пакетам, получаемым коммутатором. По умолчанию приоритет для классификации VLAN для нетегированного пакета является MAC-based > Subnet-based > Protocol VLAN.

Пример

В данном примере показано, как создать привязку VLAN ID на основе MAC-адреса для MAC-адреса 00-80-cc-00-00-11.

```
Switch# configure terminal
Switch(config)# mac-vlan 00-80-cc-00-00-11 vlan 101 priority 4
Switch(config)#
```

80-13 protocol-vlan profile

Данная команда используется для создания группы протоколов. Используйте форму **no** для удаления указанной группы протоколов.

protocol-vlan profile *PROFILE-ID* **frame-type {ethernet2 | snap | llc} ether-type** *TYPE-VALUE*
no protocol-vlan profile *PROFILE-ID*

Параметры

PROFILE-ID	VLAN ID для привязки Группа протоколов, которую следует добавить или удалить. на основе MAC-адреса.
frame-type	Тип кадров.
ethernet2	Значение для типа кадров Ethernet II.
snap	Значение для типа кадров SNAP.
llc	Значение для типа кадров LLC.
ether-type *TYPE-VALUE*	Указывает тип. Данное значение должно быть 2-байтным в шестнадцатиричной форме.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду **protocol-vlan profile** в режиме Global Configuration Mode для создания группы протоколов. Затем используйте команду **protocol-vlan profile** в режиме Interface Configuration Mode для настройки классификации VLAN для группы протоколов, получаемых на порту.

Пример

В данном примере показано, как создать VLAN-группу протоколов с идентификатором группы 10, указав, что будет использоваться протокол IPv6 (тип кадров — Ethernet2, значение - 0x86dd).

```
Switch# configure terminal
Switch(config)# protocol-vlan profile 10 frame-type ethernet2 ether-type 0x86dd
Switch(config)#
```

80-14 protocol-vlan profile (Interface)

Данная команда используется для настройки привязки VLAN для группы протоколов на порту. Используйте форму **no** для удаления привязки VLAN на порту.

protocol-vlan profile *PROFILE-ID* **vlan** *VLAN-ID* **[priority** *COS-VALUE***]**

no protocol-vlan profile *PROFILE-ID*

Параметры

PROFILE-ID	Идентификатор группы протоколов, который должен классифицироваться.
vlan *VLAN-ID*	VLAN ID для protocol VLAN. Для каждой группы привязки может быть указан только один VLAN ID.
priority *COS-VALUE*	(Опционально) Значение приоритета CoS. Если параметр не указан, то значением CoS по умолчанию является 0.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать VLAN для группы протоколов на порту. В результате, пакет, полученный на порту, который соответствует указанной группе протоколов, будет определен в указанную VLAN. VLAN не должна обязательно существовать для настройки команды. Приоритет классификации VLAN для нетегированного пакета является MAC-based > Subnet-based > Protocol VLAN.

Пример

В данном примере показано, как создать привязку VLAN на Ethernet 1/0/1 для классификации пакетов в группе протоколов 10 в VLAN 3000.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# protocol-vlan profile 10 vlan 3000
Switch(config-if)#
```

80-15 show protocol-vlan

Данная команда используется для отображения параметров настройки, касающихся protocol VLAN.

show protocol-vlan {profile [*PROFILE-ID* **[, | -]] | interface [***INTERFACE-ID* **[, | -]]}**

Параметры

profile	Группа протоколов.
PROFILE-ID	(Опционально) Группа протоколов, которая должна отображаться.
,	(Опционально) Серия идентификаторов профилей (Profile

	ID) или разделение идентификаторов профилей от предыдущего диапазона. Перед и после запятой использование пробела недопустимо.
-	(Опционально) Диапазон идентификаторов профилей. Перед дефисом и после дефиса использование пробела недопустимо.
interface	Интерфейсы, которые должны отображаться.
INTERFACE-ID	(Опционально) Порт для отображения настроек классификации protocol VLAN.
,	(Опционально) Диапазон интерфейсов или разделение интерфейсов от предыдущего диапазона. Перед и после запятой использование пробела недопустимо.
-	(Опционально) Диапазон интерфейсов. Перед дефисом и после дефиса использование пробела недопустимо.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду для отображения настроек для классификации VLAN на порту на основе группы протоколов.

Пример

В этом примере показано, как отобразить настройку для классификации VLAN на основе группы протоколов на порту 1.

```
Switch# show protocol-vlan interface eth1/0/1

 Interface       Protocol Group ID  VLAN  Priority
 --------------  -----------------  ----  --------
 eth1/0/1        10                 3000  0

Switch#
```

В данном примере показано, как отобразить настройки профиля группы протоколов.

```
Switch#show protocol-vlan profile

 Profile ID  Frame-type   Ether-type
 ----------  -----------  ----------------
 10          Ethernet2    0x86DD(IPv6)

Switch#
```

81. Команды Voice VLAN

81-1 voice vlan

Данная команда используется для глобального включения функции Voice VLAN и её настройки. Используйте форму **no**, чтобы отключить функцию Voice VLAN.

voice vlan *VLAN-ID*
no voice vlan

Параметры

VLAN-ID	Укажите VLAN ID голосовой VLAN в диапазоне от 2 до 4094.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

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 голосовые 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 голосовые 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)#
```

81-2 voice vlan aging

Данная команда используется для настройки времени устаревания (Aging Time) для устаревших динамических Member-портов Voice VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

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 голосовой трафик возобновляется в течение времени устаревания, таймер будет отменен.

Пример

В данном примере показано, как настроить время устаревания Voice VLAN на 30 минут.

```
Switch# configure terminal
Switch(config)# voice vlan aging 30
Switch(config)#
```

81-3 voice vlan enable

Данная команда используется для включения функции Voice VLAN на портах. Используйте форму **no**, чтобы отключить функцию Voice VLAN на портах.

voice vlan enable
no voice vlan enable

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда действует для портов доступа или гибридных портов. Используйте команду **voice vlan enable**, чтобы включить функцию голосовой VLAN для портов. Как команда **voice vlan** в глобальной конфигурации, так и команда **voice vlan enable** в режиме конфигурации интерфейса должны быть включены для порта, чтобы запустить функцию голосовой VLAN.

Пример

В данном примере показано, как включить функцию Voice VLAN на физическом порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# voice vlan enable
Switch(config-if)#
```

81-4 voice vlan mac-address

Данная команда используется для добавления уникального идентификатора организации (OUI), определяемого с устройства системы IP-телефонии. Используйте форму **no**, чтобы удалить OUI устройства системы IP-телефонии.

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 OUI. Максимально допустимое 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для добавления уникального идентификатора организации (OUI), определяемого с устройства системы IP-телефонии. 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.
OUI, определяемый с устройства системы IP-телефонии, не может совпадать с OUI по умолчанию. OUI по умолчанию не может быть удален.

Пример

В данном примере показано, как добавить OUI для устройства системы IP-телефонии.

```
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)#
```

81-5 voice vlan mode

Данная команда используется для включения автоматического изучения порта в качестве Member- порта Voice VLAN. Используйте форму **no**, чтобы отключить автоматическое изучение.

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

Уровень команды по умолчанию

Уровень 12

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 участника Voice VLAN. В дальнейшем участники будут автоматически удалены согласно времени устаревания. Когда порт работает в автотегированном режиме (**Auto Tagged 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 Untagged 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 Tagged Mode**) на физическом порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# voice vlan mode auto tag
Switch(config-if)#
```

81-6 voice vlan qos

Данная команда используется для настройки приоритета CoS для входящего трафика Voice VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для маркировки CoS голосовых пакетов, поступающих на порт, на котором включена Voice VLAN. Маркировка CoS позволяет отделить голосовой трафик от трафика данных по качеству обслуживания.

Пример

В данном примере показано, как настроить приоритет Voice VLAN со значением 7.

```
Switch# configure terminal
Switch(config)# voice vlan qos 7
Switch(config)#
```

81-7 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) Указывает на отображение информации о голосовой VLAN для портов.
interface *INTERFACE-ID*	(Опционально) Указывает интерфейс 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.
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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

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 данном примере 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 этом примере показано, как отобразить изученные голосовые устройства на портах 1 - 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 данном примере показано, как отобразить VoIP-устройства, обнаруженные через LLDP-MED, на Eth-портах 1/0/1-1/0/2.

```
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#
```

82. Команды Web-аутентификации

82-1 web-auth enable

Данная команда используется для включения функции Web-аутентификации на порту. Используйте форму **no**, чтобы отключить функцию Web-аутентификации.

web-auth enable
no web-auth enable

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для аутентификации узлов, подключенных к порту, через Web-браузер.

Пример

В данном примере показано, как включить функцию Web-аутентификации на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# web-auth enable
Switch(config-if)#
```

82-2 web-auth page-element

Данная команда используется для настройки элементов страницы Web-аутентификации. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

web-auth page-element {page-title *STRING* **| login-window-title** *STRING* **| username-title** *STRING* **| password-title** STRING **| logout-window-title** *STRING* **| copyright-line** *LINE-NUMBER* **title***STRING***}**
no web-auth page-element {page-title | login-window-title | username-title | password-title | logout-window-title | copyright-line}

Параметры

page-title *STRING*	Укажите заголовок страницы Web-аутентификации. Максимально допустимое количество символов – 128.

login-window-title *STRING*	Укажите заголовок окна для ввода логина/пароля страницы Web- аутентификации. Максимально допустимое количество символов – 64.
username-title *STRING*	Укажите название поля для ввода имени пользователя на странице Web- аутентификации. Максимально допустимое количество символов – 32.
password-title STRING	Укажите название поля для ввода пароля на странице Web-аутентификации. Максимально допустимое количество символов – 32.
logout-window-title *STRING*	Укажите заголовок окна выхода из системы (Logout) на странице Web- аутентификации. Максимально допустимое количество символов – 64.
copyright-line *LINE-NUMBER* **title***STRING*	Укажите информацию об авторских правах построчно на страницах Web- аутентификации. Максимально допустимое количество строк – 5. Максимально допустимое количество символов для каждой строки – 128.

По умолчанию

Заголовок страницы по умолчанию не установлен.
Заголовок окна для ввода логина/пароля по умолчанию – «Authentication Login».
Название поля для ввода имени пользователя по умолчанию – «User Name».
Название поля для ввода пароля по умолчанию – «Password».
Заголовок окна выхода из системы (Logout) по умолчанию – «Logout From The Network».
Информация об авторских правах по умолчанию не указана.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Элементы страницы Web-аутентификации могут быть настроены от имени администратора. Существуют две страницы Web-аутентификации: (1) страница входа и (2) страница выхода. Введите имя пользователя и пароль на странице входа. Используйте кнопку **Logout**, чтобы выйти из сети.

Пример

В данном примере показано, как изменить информацию об авторских правах в двух строках нижней части страницы аутентификации:

Строка 1: Copyright @ 2020 All Rights
Строка 2: Site: http://support.website.com

```
Switch# configure terminal
Switch(config)# web-auth page-element copyright-line 1 title Copyright @ 2020 All
Rights Reserved
Switch(config)# web-auth page-element copyright-line 2 title Site:
http://support.website.com
Switch(config)#
```

82-3 web-auth success redirect-path

Данная команда используется для настройки URL, на который клиент будет по умолчанию переадресован после успешной аутентификации. Используйте форму **no**, чтобы удалить указанный URL.

web-auth success redirect-path *STRING*
no web-auth success redirect-path

Параметры

STRING	Укажите URL, на который клиент будет по умолчанию переадресован после успешной аутентификации. Если URL не указан, будет отображена страница выхода Web-аутентификации. Максимально допустимое количество символов переадресации – 128.

По умолчанию

По умолчанию отображается страница выхода Web-аутентификации.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для указания Web-страницы, которую необходимо отобразить узлам, прошедшим Web-аутентификацию.

Пример

В данном примере показано, как настроить путь переадресации, который будет использован по умолчанию после прохождения Web-аутентификации. Настроенный путь – http://www.website.com.

```
Switch# configure terminal
Switch(config)# web-auth success redirect-path http://www.website.com
Switch(config)#
```

82-4 web-auth system-auth-control

Данная команда используется для глобального включения функции Web-аутентификации на коммутаторе. Используйте форму **no**, чтобы отключить функцию Web-аутентификации глобально на коммутаторе.

web-auth system-auth-control
no web-auth system-auth-control

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Включите функцию Web-аутентификации, чтобы получить доступ к сети Интернет через коммутатор. Коммутатор может выступать как в роли сервера аутентификации, выполняя аутентификацию на основе локальной базы данных, так и в роли клиента RADIUS, выполняя процесс аутентификации по протоколу RADIUS с помощью удаленного сервера RADIUS. В процессе аутентификации используется протокол HTTP или HTTPS.

Пример

В данном примере показано, как включить функцию Web-аутентификации на коммутаторе глобально.

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

82-5 web-auth virtual-ip

Данная команда используется для настройки виртуального IP-адреса Web-аутентификации, который используется для приема запросов аутентификации от узла. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

web-auth virtual-ip {ipv4 *IP-ADDRESS* **| ipv6** *IPV6-ADDRESS* **| url** *STRING***}**
no web-auth virtual-ip {ipv4 | ipv6 | url}

Параметры

ipv4 *IP-ADDRESS*	Укажите виртуальный IPv4-адрес Web-аутентификации.
ipv6 *IPV6-ADDRESS*	Укажите виртуальный IPv6-адрес Web-аутентификации.
url *STRING*	Укажите FQDN URL для Web-аутентификации. Максимально допустимое количество символов – 128.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Виртуальный IP-адрес является характеристикой функции Web-аутентификации на коммутаторе. Все процессы Web-аутентификации взаимодействуют с данным IP-адресом. Однако из-за того, что виртуальный IP-адрес не отвечает ни на один пакет ICMP или запрос ARP, настройка виртуального IP- адреса в той же подсети, что и IP-адреса интерфейса коммутатора или подсети узла недопустима. В противном случае, функция Web-аутентификация будет работать некорректно.

Перед использованием указанного URL необходимо настроить виртуальный IP-адрес. Чтобы получить виртуальный IP-адрес, используйте FQDN URL, который хранится на DNS-сервере. Полученный IP- адрес должен соответствовать виртуальному IP-адресу, настроенному с помощью команды. Если IPv4 или IPv6-адрес не настроен, Web-аутентификация невозможна.

Пример

В данном примере показано, как настроить виртуальный IPv4 и FQDN URL для Web-аутентификации. Настроенный IPv4-адрес – 1.1.1.1. Настроенный FQDN URL – www.website4.co.

```
Switch# configure terminal
Switch(config)# web-auth virtual-ip  ipv4 1.1.1.1
Switch(config)# web-auth virtual-ip  url www.website4.co
Switch(config)#
```

В данном примере показано, как настроить виртуальный IPv6 и FQDN URL для Web-аутентификации. Настроенный IPv6-адрес – 2000::2. Настроенный FQDN URL – www.website6.co.

```
Switch# configure terminal
Switch(config)# web-auth virtual-ip ipv6 2000::2
Switch(config)# web-auth virtual-ip url www.website6.co
Switch(config)#
```

82-6 snmp-server enable traps web-auth

Данная команда используется для включения отправки SNMP-уведомлений для Web-аутентификации. Используйте форму **no**, чтобы отключить отправку SNMP-уведомлений.

snmp-server enable traps web-auth
no snmp-server enable traps web-auth

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте эту команду, чтобы включить или отключить отправку SNMP-уведомлений для Web-аутентификации.

Пример

В данном примере показано, как включить отправку SNMP-уведомлений для Web-аутентификации.

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

Приложение A - Записи системного журнала

В следующей таблице перечислены все возможные записи и их соответствующие значения, которые будут отображаться в системном журнале данного коммутатора.

802.1X

Описание записей журнала	Уровень
Описание события: Сбой аутентификации 802.1X. Сообщение журнала: Сбой проверки подлинности 802.1X [из-за <причины>] с (Имя пользователя: <username>, <interface-id>, MAC: <mac-address>) Параметры Описание: reason: Причина неудачной аутентификации. Возможными причинами могут быть: (1) user authentication failure. (2) no server(s) responding. (3) no servers configured. (4) no resources. (5) user timeout expired. имя пользователя: пользователь, проходящий аутентификацию. interface-id: Номер интерфейса коммутатора. mac-адрес: MAC-адрес аутентифицируемого устройства.	Критический
Описание события: Аутентификация 802.1X успешна. Сообщение журнала: 802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>) Параметры Описание: имя пользователя: пользователь, который проходит проверку подлинности. interface-id: Имя интерфейса. mac-адрес: MAC-адрес аутентифицируемого устройства.	Информационный

AAA

Описание записей журнала	Уровень
Описание события: Этот журнал будет создан, когда глобальное состояние AAA включено или отключено. Сообщение журнала: AAA - <статус> Параметры Описание: status: Статус указывает на то, что AAA включен или отключен.	Информационный
Описание события: Этот журнал будет создан при успешном входе в систему. Сообщение журнала: Успешный вход через <exec-type> [from <client-ip>] authenticated by AAA <aa-method> <server-ip> (Username: <username>).	Предупреждение

Параметры Описание: exec-type: Указывает типы EXEC, например: Console, Telnet, SSH, Web, Web(SSL). client-ip: Указывает IP-адрес клиента, если он действителен по протоколу IP. aaa-method: Указывает метод аутентификации, например: нет, локальный, сервер. server-ip: Указывает IP-адрес сервера AAA, если метод аутентификации - удаленный сервер. Имя пользователя: Указывает имя пользователя для аутентификации.	
Описание события: Этот журнал генерируется, когда удаленный сервер не отвечает на запрос аутентификации входа. Сообщение журнала: Не удалось войти в систему через <exec-type> [с <client-ip>] из-за тайм-аута сервера AAA <server-ip> (Имя пользователя: <username>) Параметры Описание: exec-type: Указывает типы EXEC, например: Console, Telnet, SSH, Web, Web(SSL). client-ip: Указывает IP-адрес клиента, если он действителен по протоколу IP. server-ip: Указывает IP-адрес сервера AAA. имя пользователя: Указывает имя пользователя для аутентификации.	Предупреждение
Описание события: Этот журнал будет создан при успешном включении привилегии. Сообщение журнала: Успешное включение привилегий через <exec-type> [from <client- ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>). Параметры Описание: exec-type: Указывает типы EXEC, например: Console, Telnet, SSH, Web, Web(SSL). client-ip: Указывает IP-адрес клиента, если он действителен по протоколу IP. aaa-method: Указывает метод аутентификации, например: нет, локальный, сервер. server-ip: Указывает IP-адрес сервера AAA, если метод аутентификации - удаленный сервер. Имя пользователя: Указывает имя пользователя для аутентификации.	Информационный
Описание события: Этот журнал будет создан при отказе привилегий. Сообщение журнала: Не удалось включить привилегию через <exec-type> [from <client-ip>] authenticated by AAA <aa-method> <server-ip> (Username: <username>). Параметры Описание: exec-type: Указывает типы EXEC, например: Console, Telnet, SSH, Web, Web(SSL). client-ip: Указывает IP-адрес клиента, если он действителен	Предупреждение

по протоколу IP. aaa-method: Указывает метод аутентификации, например: локальный, серверный. server-ip: Указывает IP-адрес сервера AAA, если метод аутентификации - удаленный сервер. имя пользователя: Указывает имя пользователя для аутентификации.	
Описание события: Этот журнал генерируется, когда удаленный сервер не отвечает на запрос аутентификации с включенным паролем. Сообщение журнала: Enable privilege failed through <exec-type> [from <client-ip>] due to AAA server <server-ip> timeout (Username: <username>). Параметры Описание: exec-type: Указывает типы EXEC, например: Console, Telnet, SSH, Web, Web(SSL). client-ip: Указывает IP-адрес клиента, если он действителен по протоколу IP. server-ip: Указывает IP-адрес сервера AAA. имя пользователя: Указывает имя пользователя для аутентификации.	Предупреждение
Описание события: Этот журнал генерируется, когда RADIUS назначает действительные атрибуты VLAN ID. Сообщение журнала: Сервер RADIUS <server-ip> назначил VID: <vid> порту <interface-id> (Имя пользователя: <username>). Параметры Описание: server-ip: Указывает IP-адрес сервера RADIUS. vid: Назначение VLAN ID, авторизованного сервером RADIUS. Interface-id: Указывает номер порта клиента, прошедшего аутентификацию. Имя пользователя: Указывает имя пользователя для аутентификации.	Информационный
Описание события: Этот журнал будет создан, когда RADIUS назначит действительные атрибуты пропускной способности. Сообщение журнала: Сервер RADIUS <server-ip> назначил <направление> полосы пропускания: <порог> порту <interface-id> (Имя пользователя: <username>). Параметры Описание: server-ip: Указывает IP-адрес сервера RADIUS. Направление: Указывает направление контроля полосы пропускания, например: вход или выход. Threshold (порог): Назначение порога пропускной способности, разрешенной сервером RADIUS. Interface-id: Указывает номер порта клиента, прошедшего аутентификацию. Имя пользователя: Указывает имя пользователя для аутентификации.	Информационный
Описание события: Этот журнал будет создан, когда RADIUS назначит действительные атрибуты приоритета. Сообщение журнала: Сервер RADIUS <server-ip> назначил приоритет 802.1p по умолчанию: <приоритет> порту <интерфейс -id> (Имя пользователя: <имя пользователя>).	Информационный

Параметры Описание: server-ip: Указывает IP-адрес сервера RADIUS. приоритет: Назначение приоритета, авторизованного сервером RADIUS. interface-id: Указывает номер порта клиента для аутентификации. Имя пользователя: Указывает имя пользователя для аутентификации.	
Описание события: Этот журнал будет создан, когда RADIUS назначил сценарий ACL, но не смог применить его к системе из-за недостаточного ресурса. Сообщение журнала: RADIUS сервер <server-ip> назначает <имя пользователя> ACL сбой на порту <interface-id> (<acl-script>). Параметры Описание: server-ip: Указывает IP-адрес сервера RADIUS. username: Указывает имя пользователя для аутентификации. interface-id: Указывает номер порта клиента для аутентификации. acl-script: Назначение ACL-скрипта, авторизованного сервером RADIUS.	Предупреждение
Описание события: Этот журнал будет создан, когда назначенный RADIUS сценарий ACL будет применен к системе из-за недостаточного ресурса. Сообщение журнала: RADIUS сервер <server-ip> назначает <имя пользователя> ACL успех на порту <интерфейс -id> (<acl-script>). Параметры Описание: server-ip: Указывает IP-адрес сервера RADIUS. username: Указывает имя пользователя для аутентификации. interface-id: Указывает номер порта клиента для аутентификации. acl-script: Назначение ACL-скрипта, авторизованного сервером RADIUS.	Информационный

ARP Spoofing Prevention

Описание записей журнала	**Уровень**
Описание события: поддельный ARP-пакет обнаружен системой ARP Spoofing Prevention. Сообщение журнала: Шлюз <ipaddr> атакован <macaddr> с <interface-id>. Параметры Описание: ipaddr: IP-адрес шлюза. macaddr: MAC-адрес хакера. interface-id: Интерфейс, на котором находится хакер.	Предупреждение

Auto Save Configuration

Описание записей журнала	**Уровень**
Описание события: Запись события, когда информация конфигурации ddp сохраняется автоматически.	Информационный

Сообщение журнала:CONFIG-6-DDPSAVECONFIG: [Unit <unitID>,]Конфигурация автоматически сохраняется во флэш-памяти из-за конфигурирования из DDP (Username: <username>, IP: <ipaddr>). Параметры Описание: Unit: ID блока. имя пользователя: Представляет текущего пользователя входа в систему. ipaddr: Представляет IP-адрес клиента.	

Auto Surveillance VLAN

Описание записей журнала	**Уровень**
Описание события: При обнаружении нового устройства наблюдения на интерфейсе. Сообщение журнала: Обнаружено новое устройство наблюдения (<interface-id>, MAC: <mac-адрес>). Параметры Описание: interface-id: Имя интерфейса. mac-адрес: MAC-адрес устройства наблюдения.	Информационный
Описание события: Когда интерфейс, на котором включена сеть наблюдения VLAN, автоматически присоединяется к сети наблюдения VLAN. Log Message: <interface-id> add into surveillance VLAN <vid> Parameters Description: interface-id: Имя интерфейса. vid:Идентификатор виртуальной локальной сети.	Информационный
Описание события: Когда интерфейс покидает VLAN наблюдения и в то же время в интервале старения для этого интерфейса не обнаружено ни одного устройства наблюдения, будет отправлено сообщение журнала. Сообщение журнала: <interface-id> remove from surveillance VLAN <vid> Описание параметров: interface-id: Имя интерфейса. vid:Идентификатор виртуальной локальной сети.	Информационный
Описание события: Когда IPC добавляется в VLAN наблюдения, отправляется сообщение журнала. Сообщение журнала: ASV: Add IPC(<ipaddr>) Описание параметров: ipaddr: Представляет собой IP-адрес IPC.	Информационный
Описание события: Когда IPC удаляется из сети наблюдения VLAN, отправляется сообщение журнала. Сообщение журнала: ASV: Remove IPC(<ipaddr>) Параметры Описание: ipaddr: Представляет собой IP-адрес IPC.	Информационный
Описание события: Когда NVR добавляется в сеть VLAN наблюдения, отправляется сообщение журнала. Сообщение журнала: ASV: Add NVR(<ipaddr>) Описание параметров: ipaddr: Представляет собой IP-адрес сетевого видеорегистратора.	Информационный

Описание события: Когда сетевой видеорегистратор удаляется из сети наблюдения VLAN, отправляется сообщение журнала. Сообщение журнала: ASV: Remove NVR(<ipaddr>) Параметры Описание: ipaddr: Представляет собой IP-адрес сетевого видеорегистратора.	Информационный
Описание события: Когда режим ASV 2.0 изменяется с помощью Web GUI, отправляется сообщение журнала. Сообщение журнала: ASV: Изменение режима с <mode> на <mode> Описание параметров: mode: Представляет собой режим ASV 2.0. Режим может быть стандартным или режимом наблюдения.	Информационный

BPDU Attack Protection

Описание записей журнала	**Уровень**
Описание события: Запишите событие, когда произошла атака BPDU. Log Message: <interface-id> enter STP BPDU under protection state (mode: <mode>) Параметры Описание: interface-id: Интерфейс, на котором обнаружена атака STP BPDU. mode: Режим защиты BPDU интерфейса. Режим может быть drop, block или shutdown.	Информационный
Описание события: Запись события, когда атака STP BPDU восстановилась. Log Message: <interface-id> recover from BPDU under protection state Параметры Описание: interface-id: Интерфейс, на котором обнаружена атака STP BPDU.	Информационный

Configuration/Firmware

Описание записей журнала	**Уровень**
Описание события: Прошивка успешно обновлена. Сообщение журнала: [Unit <unitID>,]Firmware upgraded by <session> successfully (Username: <имя пользователя>[, IP: <ipaddr>, MAC: <macaddr>], IP сервера: <serverIP>, Имя файла: <pathFile>) Параметры Описание: unitID: идентификатор устройства. сессия: Сеанс пользователя. имя пользователя: Представляет текущего пользователя. ipaddr: Представляет IP-адрес клиента. macaddr : Представляет MAC-адрес клиента. serverIP: IP-адрес сервера. pathFile: Путь и имя файла на сервере.	Информационный
Описание события: Неудачное обновление микропрограммы. Сообщение журнала: [Unit <unitID>,]Firmware upgraded by <session> unsuccessfully (Username: <имя пользователя>[, IP:	Предупреждение

<ipaddr>, MAC: <macaddr>], IP сервера: <serverIP>, Имя файла: <pathFile>) Параметры Описание: unitID: идентификатор устройства. сессия: Сеанс пользователя. имя пользователя: Представляет текущего пользователя. ipaddr: Представляет IP-адрес клиента. macaddr : Представляет MAC-адрес клиента. serverIP: IP-адрес сервера. pathFile: Путь и имя файла на сервере.	
Описание события: Прошивка загружена успешно. Сообщение в журнале: [Unit <unitID>,]Firmware uploaded by <session> successfully (Username: <имя пользователя>[, IP: <ipaddr>, MAC: <macaddr>], IP сервера: <serverIP>, Имя файла: <pathFile>) Параметры Описание: unitID: идентификатор устройства. сессия: Сеанс пользователя. имя пользователя: Представить текущего пользователя для входа в систему. ipaddr: IP-адрес клиента. macaddr : Представляет MAC-адрес клиента. serverIP: IP-адрес сервера. pathFile: Путь и имя файла на сервере.	Информационный
Описание события: Неудачная загрузка микропрограммы. Сообщение журнала: [Unit <unitID>,]Firmware uploaded by <session> unsuccessfully (Username: <имя пользователя>[, IP: <ipaddr>, MAC: <macaddr>], IP сервера: <serverIP>, Имя файла: <pathFile>) Параметры Описание: unitID: идентификатор устройства. сессия: Сеанс пользователя. имя пользователя: Представляет текущего пользователя. ipaddr: IP-адрес клиента. macaddr : Представляет MAC-адрес клиента. serverIP: IP-адрес сервера. pathFile: Путь и имя файла на сервере.	Предупреждение
Описание события: Конфигурация загружена успешно. Сообщение журнала: [Unit <unitID>,]Конфигурация загружена <session> успешно. (Имя пользователя: <имя пользователя>[, IP: <ipaddr>, MAC: <macaddr>], IP сервера: <serverIP>, Имя файла: <pathFile>) Параметры Описание: unitID: идентификатор устройства. сессия: Сеанс пользователя. имя пользователя: Представляет текущего пользователя. ipaddr: Представляет IP-адрес клиента. macaddr : Представляет MAC-адрес клиента. serverIP: IP-адрес сервера. pathFile: Путь и имя файла на сервере.	Информационный
Описание события: Конфигурация загружена неудачно. Сообщение журнала: [Unit <unitID>,]Конфигурация загружена <session> неудачно. (Имя пользователя: <имя	Предупреждение

пользователя>[, IP: <ipaddr>, MAC: <macaddr>], IP сервера: <serverIP>, Имя файла: <pathFile>) Параметры Описание: unitID: идентификатор устройства. сессия: Сеанс пользователя. имя пользователя: Представляет текущего пользователя. ipaddr: Представляет IP-адрес клиента. macaddr : Представляет MAC-адрес клиента. serverIP: IP-адрес сервера. pathFile: Путь и имя файла на сервере.	
Описание события: Конфигурация загружена успешно. Сообщение журнала: [Unit <unitID>,]Configuration uploaded by <session> successfully. (Имя пользователя: <имя пользователя>[, IP: <ipaddr>, MAC: <macaddr>], IP сервера: <serverIP>, Имя файла: <pathFile>) Параметры Описание: unitID: идентификатор устройства. сессия: Сеанс пользователя. имя пользователя: Представляет текущего пользователя. ipaddr: Представляет IP-адрес клиента. macaddr : Представляет MAC-адрес клиента. serverIP: IP-адрес сервера. pathFile: Путь и имя файла на сервере.	Информационный
Описание события: Конфигурация загружена неудачно. Log Message: [Unit <unitID>,]Конфигурация загружена <session> неудачно. (Имя пользователя: <имя пользователя>[, IP: <ipaddr>, MAC: <macaddr>], IP сервера: <serverIP>, Имя файла: <pathFile>) Параметры Описание: unitID: идентификатор устройства. сессия: Сеанс пользователя. имя пользователя: Представляет текущего пользователя. ipaddr: Представляет IP-адрес клиента. macaddr : Представляет MAC-адрес клиента. serverIP: IP-адрес сервера. pathFile: Путь и имя файла на сервере.	Предупреждение
Описание события: Конфигурация сохранена во флэш-память с помощью консоли. Сообщение в журнале: [Unit <unitID>,] Configuration saved to flash by console (Username: <username>) Параметры Описание: unitID: идентификатор устройства. имя пользователя: Представить текущего пользователя для входа в систему.	Информационный
Описание события: Конфигурация сохранена во флэш-память удаленным устройством. Log Message: [Unit <unitID>,]Configuration saved to flash (Username: <username>, IP: <ipaddr>) Параметры Описание: unitID: идентификатор устройства. имя пользователя: Представляет текущего пользователя для	Информационный

входа в систему. ipaddr: IP-адрес клиента.	
Описание события: Сообщение журнала успешно загружено. Сообщение журнала: [Unit <unitID>,] Сообщение журнала загружено <session> успешно. (Имя пользователя: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Параметры Описание: unitID: идентификатор устройства. session: Сеанс пользователя. имя пользователя: Представляет текущего пользователя. ipaddr: Представляет IP-адрес клиента. macaddr: Представляет MAC-адрес клиента.	Информационный
Описание события: Сообщение журнала загружено неудачно. Сообщение журнала: [Unit <unitID>,] Сообщение журнала загружено <сессией> неудачно. (Имя пользователя: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Параметры Описание: unitID: идентификатор устройства. сессия: Сеанс пользователя. имя пользователя: Представить текущего пользователя для входа в систему. ipaddr: Представляет IP-адрес клиента. macaddr: Представляет MAC-адрес клиента.	Предупреждение
Описание события: Неудачно загружены файлы неизвестного типа. Сообщение журнала: [Unit <unitID>,]Downloaded by <session> unsuccessfully. (Имя пользователя: <имя пользователя>[, IP: <ipaddr>, MAC: <macaddr>], IP сервера: <serverIP>, Имя файла: <pathFile>) Параметры Описание: unitID: идентификатор устройства. сессия: Сеанс пользователя. имя пользователя: Представить текущего пользователя для входа в систему. ipaddr: Представляет IP-адрес клиента. macaddr : Представляет MAC-адрес клиента. serverIP: IP-адрес сервера. pathFile: Путь и имя файла на сервере.	Предупреждение

DAI

Описание записей журнала	**Уровень**
Описание события: Этот журнал создается, когда DAI обнаруживает недействительный ARP-пакет. Сообщение журнала: Нелегальные ARP <тип> пакеты (IP: <ip-address>, MAC: <mac- address>, VLAN <vlan-id>, on <interface-id>). Параметры Описание:	Предупреждение

type: Тип ARP-пакета, он указывает на то, что ARP-пакет является запросом или ARP-ответом.	
Описание события: Этот журнал будет создан, когда DAI обнаружит действительный ARP-пакет. Сообщение журнала: Законные ARP <тип> пакеты (IP: <ip-address>, MAC: <mac- address>, VLAN <vlan-id>, on <interface-id>). Параметры Описание: type: Тип ARP-пакета, он указывает, является ли ARP-пакет запросом или ARP-ответом.	Информационный

DDM

Описание записей журнала	**Уровень**
Описание события: когда любой из параметров SFP превышает порог предупреждения. Сообщение журнала: Превышен порог предупреждения оптического трансивера <interface-id> <component> <high-low>. Параметры Описание: interface-id: идентификатор интерфейса порта. component (компонент): Тип порога DDM. Он может быть одним из следующих типов: temperature supply voltage bias current TX power RX power high-low: Высокий или низкий порог.	Предупреждение
Описание события: когда любой из параметров SFP превышает порог тревоги. Сообщение журнала: Превышен порог тревоги оптического трансивера <interface-id> <component> <high-low>. Параметры Описание: interface-id: идентификатор интерфейса порта. компонент: Тип порога DDM. Он может быть одним из следующих типов: temperature (температура) supply voltage bias current TX power RX power high-low: Высокий или низкий порог.	Критический
Описание события: когда любой из параметров SFP восстанавливается после порога предупреждения. Сообщение журнала: Оптический трансивер <interface-id> <компонент> вернулся в нормальное состояние. Описание параметров:	Предупреждение

interface-id: идентификатор интерфейса порта. компонент: Тип порога DDM. Он может быть одним из следующих типов: temperature ("температура") supply voltage bias current TX power RX power	

DHCPv6 Client

Описание записей журнала	**Уровень**
Описание события: Изменено состояние администратора интерфейса клиента DHCPv6. Сообщение журнала: Клиент DHCPv6 на интерфейсе <ipif-name> изменил состояние на [enabled | disabled]. Параметры Описание: <ipif-name>: имя интерфейса клиента DHCPv6.	Информационный
Описание события: Клиент DHCPv6 получает ipv6-адрес от сервера DHCPv6. Сообщение журнала: Клиент DHCPv6 получает ipv6-адрес <ipv6address> на интерфейсе <ipif-name>. Параметры Описание: ipv6address: ipv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса клиента DHCPv6.	Информационный
Описание события: ipv6-адрес, полученный от сервера DHCPv6, начинает обновляться. Сообщение журнала: IPv6-адрес <ipv6address> на интерфейсе <ipif-name> начинает обновляться. Параметры Описание: ipv6address: ipv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса клиента DHCPv6.	Информационный
Описание события: ipv6-адрес, полученный от сервера DHCPv6, успешно обновляется. Сообщение журнала: IPv6-адрес <ipv6address> на интерфейсе <ipif-name> обновлен успешно. Параметры Описание: ipv6address: ipv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса клиента DHCPv6.	Информационный
Описание события: ipv6-адрес, полученный от сервера DHCPv6, начинает переприязку. Сообщение журнала: IPv6-адрес <ipv6address> на интерфейсе <ipif-name> начинает переприязку. Параметры Описание: ipv6address: ipv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса клиента DHCPv6.	Информационный
Описание события: Адрес ipv6, полученный от сервера	Информационный

DHCPv6, успешно перепривязан. Сообщение журнала: IPv6-адрес <ipv6address> на интерфейсе <ipif-name> rebinds success. Параметры Описание: ipv6address: ipv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса клиента DHCPv6.	
Описание события: Удален ipv6-адрес с сервера DHCPv6. Сообщение журнала: IPv6-адрес <ipv6address> на интерфейсе <ipif-name> был удален. Описание параметров: ipv6address: ipv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса клиента DHCPv6.	Информационный

DHCPv6 Relay

Описание записей журнала	**Уровень**
Описание события: Изменено состояние администратора ретрансляции DHCPv6 на указанном интерфейсе. Сообщение журнала: DHCPv6 relay on interface <ipif-name> changed state to [enabled | disabled]. Параметры Описание: <ipif-name>: имя интерфейса агента ретрансляции DHCPv6.	Информационный

DNS Resolver

Описание записей журнала	**Уровень**
Event Description: Duplicate Domain name cache added, leads a dynamic domain name cache be deleted. Log Message: Duplicate Domain name case name: <domainname>, static IP: <ipaddr>, dynamic IP:<ipaddr> Parameters Description: domainname: the domain name string. ipaddr: IP address.	Информационный

DoS Prevention

Описание записей журнала	**Уровень**
Описание события: Обнаружение DOS-атаки. Log Message: <dos-type> сброшен с (IP: <ip-address> Port <interface- id>). Параметры Описание: dos-type: тип DOS-атаки ip-адрес: IP-адрес. interface-id: Имя интерфейса	Уведомление

Errdisable

Описание записей журнала	**Уровень**

Описание события: Когда порт входит в состояние отключения при ошибке. Сообщение журнала: Порт <interface-id> входит в состояние отключения из-за ошибки по <reason- id>. Описание параметров: interface-id: Номер порта. reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, Digital Diagnostics Monitoring, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving.	Предупреждение
Описание события: Когда порт выходит из состояния отключения при ошибке. Сообщение журнала: Порт <interface-id> выходит из состояния отключения ошибок, которое ранее было вызвано <reason-id>. Параметры Описание: interface-id: Номер порта. reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, Digital Diagnostics Monitoring, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving.	Предупреждение
Описание события: Когда порт входит в состояние отключения при ошибке. Log Message: Порт <interface-id> VLAN <vid> вошел в состояние отключения из-за ошибки <reason-id>. Параметры Описание: interface-id: Номер порта. reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, Digital Diagnostics Monitoring, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving. vid:vlan id	Предупреждение
Описание события: Когда порт выходит из состояния отключения при ошибке. Log Message: Порт <interface-id> VLAN <vid> выходит из состояния отключения ошибок, которое ранее было вызвано <reason-id>. reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, Digital Diagnostics Monitoring, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving. vid:vlan id	Предупреждение

Interface

Описание записей журнала	**Уровень**
Описание события: Когда порт не работает. Log Message: Порт <port-type> <interface-id> link down Параметры Описание:	Информационный

port-type: тип порта interface-id: имя интерфейса	
Описание события: Когда порт находится в рабочем состоянии. Log Message: Порт <port-type> <interface-id> link up, <link-speed> Параметры Описание: port-type: тип порта interface-id: имя интерфейса link-speed: скорость соединения порта.	Информационный
Описание события: Порт связан в полудуплексном режиме. Log Message: ASV: Port <interface-id> Half duplex detected Parameters Description: Параметры Описание: interface-id: Номер порта. interface-id: Имя интерфейса	Информационный

JWAC

Описание записей журнала	**Уровень**
Описание события: когда хост прошел аутентификацию. Сообщение журнала: JWAC host login success (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <mac-адрес>, <interface-id>, VID: <vlan-id>) Параметры Описание: Имя пользователя: Имя пользователя хоста. IP: IP-адрес хоста mac-адрес: MAC-адреса хоста. interface-id: Интерфейс, на котором хост аутентифицирован. vlan-id: Идентификатор виртуальной локальной сети, в которой существует хост.	Информационный
Описание события: Когда хост не проходит аутентификацию. Сообщение журнала: JWAC host login fail (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <mac-адрес>, <interface-id>, VID: <vlan-id>) Параметры Описание: Имя пользователя: имя пользователя хоста. IP: IP-адрес хоста mac-адрес: MAC-адрес хоста. interface-id: Интерфейс, на котором хост аутентифицирован. vlan-id: Идентификатор виртуальной локальной сети, в которой существует хост.	Критический
Описание события: когда количество авторизованных пользователей на всем устройстве достигло максимального предела. Сообщение журнала: JWAC переходит в состояние остановки обучения	Предупреждение
Описание события: когда количество авторизованных	Предупреждение

пользователей на всем устройстве ниже максимального предела пользователей в течение определенного интервала времени. Сообщение журнала: JWAC восстанавливается из состояния остановки обучения	

LACP

Описание записей журнала	**Уровень**
Описание события: Link Aggregation Group link up. Сообщение журнала: Link Aggregation Group <group_id> link up Параметры Описание: group_id: Идентификатор группы агрегации каналов.	Информационный
Описание события: Неисправность соединения группы агрегации каналов. Сообщение журнала: Link Aggregation Group <group_id> link down Параметры Описание: group_id: Идентификатор группы агрегации каналов.	Информационный
Описание события: Порт-член присоединен к группе агрегации каналов. Log Message: <ifname> attach to Link Aggregation Group <group_id> Параметры Описание: ifname: имя интерфейса порта, который присоединяется к группе агрегации. group_id: Идентификатор группы агрегации, к которой присоединяется порт.	Информационный
Описание события: Порт-член отсоединяется от группы агрегации каналов. Log Message: <ifname> detach from Link Aggregation Group <group_id> Параметры Описание: ifname: имя интерфейса порта, который отсоединяется от группы агрегации. group_id: Идентификатор группы агрегации, от которой отсоединяется порт.	Информационный

LBD

Описание записей журнала	**Уровень**
Описание события: Запись события, когда интерфейс обнаруживает петлю. Log Message: <interface-id> LBD loop occurred Описание параметров: interface-id: Интерфейс, на котором обнаружена петля.	Критический
Описание события: Запись события, когда интерфейс обнаруживает петлю. Log Message: <interface-id> VLAN <vlan-id> LBD loop occurred Описание параметров: interface-id: Интерфейс, на котором обнаружена петля. vlan-id: VLAN, в которой обнаружена петля.	Критический
Описание события: Запись события при восстановлении петли интерфейса. Log Message: <interface-id> LBD loop	Критический

recovered Описание параметров: interface-id: Интерфейс, на котором обнаружена петля.	
Описание события: Запись события при восстановлении петли интерфейса. Log Message: <interface-id> VLAN <vlan-id> LBD loop recovered Параметры Описание: interface-id: Интерфейс, на котором обнаружена петля. vlan-id: VLAN, в которой обнаружена петля.	Критический
Описание события: Запись события, когда количество VLAN, в которых произошла петля возврата, превышает зарезервированное число. Сообщение журнала: Переполнение номеров виртуальных локальных сетей	Критический

LLDP-MED

Описание записей журнала	**Уровень**
Описание события: Обнаружено изменение топологии LLDP-MED. Сообщение журнала: Обнаружено изменение топологии LLDP-MED (на порту <portNum>. идентификатор шасси: <chassisType>, <chassisID>, идентификатор порта: <portType>, <portID>, класс устройства: <deviceClass>) Параметры Описание: portNum: Номер порта. chassisType: chassis ID subtype. Список значений: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: chassis ID. portType: port ID subtype. Список значений: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: идентификатор порта. deviceClass: Тип устройства LLDP-MED.	Уведомление
Описание события: Обнаружен конфликтный тип устройства	Уведомление

LLDP-MED. Сообщение журнала: Обнаружен конфликт типа устройства LLDP-MED (на порту <portNum>, идентификатор шасси: <chassisType>, <chassisID>, идентификатор порта: <portType>, <portID>, класс устройства: <deviceClass>) Параметры Описание: portNum: Номер порта. chassisType: chassis ID subtype. Список значений: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: chassis ID subtype. portType: port ID subtype. Список значений: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: идентификатор порта. deviceClass: Тип устройства LLDP-MED.	
Описание события: Обнаружен несовместимый набор TLV LLDP-MED. Сообщение журнала: Обнаружен несовместимый набор LLDP-MED TLV (на порту <portNum>, идентификатор шасси: <chassisType>, <chassisID>, идентификатор порта: <portType>, <portID>, класс устройства: <deviceClass>) Параметры Описание: portNum: Номер порта. chassisType: chassis ID subtype. Список значений: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: ichassis ID. portType: port ID subtype Список значений: 1. interfaceAlias(1) 2. portComponent(2)	Уведомление

3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: идентификатор порта. deviceClass: Тип устройства LLDP-MED.

Login/Logout CLI

Описание записей журнала	**Уровень**
Описание события: Вход в систему через консоль успешно выполнен. Log Message: [Unit <unitID>,]Успешный вход в систему через консоль (имя пользователя: <username>) Параметры Описание: unitID: идентификатор устройства. имя пользователя: Представляет текущего пользователя для входа в систему.	Информационный
Описание события: Неудачный вход в систему через консоль. Log Message: [Unit <unitID>,] Вход в систему через консоль не удался (имя пользователя: <username>). Параметры Описание: unitID: идентификатор устройства. username (имя пользователя): Представить текущего пользователя для входа в систему.	Предупреждение
Описание события: Консольный сеанс завершен по таймеру. Сообщение журнала: [Unit <unitID>,] Console session timed out (Username: <username>) Параметры Описание: unitID: идентификатор устройства. username (имя пользователя): Представить текущего пользователя для входа в систему.	Информационный
Описание события: Выход из системы через консоль. Сообщение в журнале: [Unit <unitID>,] Выход из системы через консоль (имя пользователя: <username>). Параметры Описание: unitID: идентификатор устройства. имя пользователя: Представить текущего пользователя входа в систему.	Информационный
Описание события: Вход в систему через telnet успешно выполнен. Сообщение журнала: Успешный вход в систему через Telnet (Имя пользователя: <username>, IP: <ipaddr>) Параметры Описание: username: Представляет текущего пользователя входа в систему.	Информационный

ipaddr: IP-адрес клиента.	
Описание события: Неудачный вход в систему через telnet. Сообщение журнала: Не удалось войти в систему через Telnet (имя пользователя: <username>, IP: <ipaddr>). Параметры Описание: имя пользователя: Представляет текущего пользователя входа в систему. ipaddr: Представляет IP-адрес клиента.	Предупреждение
Описание события: Сессия Telnet завершилась по таймеру. Сообщение журнала: Сессия Telnet завершилась (имя пользователя: <username>, IP: <ipaddr>). Параметры Описание: username (имя пользователя): Представляет текущего пользователя входа в систему. ipaddr: Представляет IP-адрес клиента.	Информационный
Описание события: Выход из системы через telnet. Сообщение журнала: Выход из системы через Telnet (имя пользователя: <username>, IP: <ipaddr>) Параметры Описание: username: Представляет текущего пользователя входа в систему. ipaddr: Представляет IP-адрес клиента.	Информационный
Описание события: Успешный вход в систему через SSH. Сообщение в журнале: Успешный вход через SSH (Имя пользователя: <username>, IP: <ipaddr>) Параметры Описание: username: Представляет текущего пользователя для входа в систему. ipaddr: IP-адрес клиента.	Информационный
Описание события: Неудачный вход в систему через SSH. Сообщение в журнале: Вход через SSH не удался (Имя пользователя: <username>, IP: <ipaddr>). Параметры Описание: username: Представляет текущего пользователя входа в систему. ipaddr: Представляет IP-адрес клиента.	Критический
Описание события: Сессия SSH завершилась по таймеру. Сообщение в журнале: Сессия SSH завершилась (имя пользователя: <username>, IP: <ipaddr>). Параметры Описание: username: Представляет текущего пользователя для входа в систему. ipaddr: Представляет IP-адрес клиента.	Информационный
Описание события: Выход из системы через SSH. Сообщение журнала: Выход из системы через SSH (имя пользователя: <username>, IP: <ipaddr>). Параметры Описание:	Информационный

username: Представляет текущего пользователя входа в систему. ipaddr: Представляет IP-адрес клиента.	

MAC-based Access Control

Описание записей журнала	**Уровень**
Описание события: Хост прошел аутентификацию. Сообщение журнала: MAC-based Access Control host login success (MAC: <mac- address>, <interface-id>, VID: <vlan-id>) Параметры Описание: mac-адрес: MAC-адрес хоста interface-id: Интерфейс, на котором хост проходит аутентификацию vlan-id: Идентификатор виртуальной локальной сети, в которой находится хост после аутентификации.	Информационный
Описание события: Хост вышел из строя. Сообщение журнала: Хост управления доступом на основе MAC вышел из строя (MAC: <mac-адрес>, <interface-id>, VID: <vlan-id>). Параметры Описание: mac-адрес: MAC-адрес хоста interface-id: Интерфейс, на котором хост аутентифицирован vlan-id: ID VLAN, в которой существует хост до того, как он будет исключен из сети.	Информационный
Описание события: Хост не прошел аутентификацию. Сообщение журнала: MAC-based Access Control host login fail (MAC: <mac- address>, <interface-id>, VID: <vlan-id>). Параметры Описание: mac-адрес: MAC-адрес хоста interface-id: Интерфейс, на котором хост проходит аутентификацию vlan-id: Идентификатор VLAN, в которой существует хост.	Критический
Описание события: Число авторизованных пользователей на всем устройстве достигло максимального предела. Сообщение журнала: Управление доступом на основе MAC переходит в состояние остановки обучения	Предупреждение
Описание события: Количество авторизованных пользователей на всем устройстве ниже максимального лимита пользователей за определенный промежуток времени. Сообщение журнала: Управление доступом на основе MAC восстанавливается из состояния остановки обученияПредупреждение	Предупреждение
Описание события: Число авторизованных пользователей на интерфейсе достигло максимального предела. Log Message: <интерфейс-id> входит в состояние остановки обучения управления доступом на основе MAC-адресов	Предупреждение

Описание параметров: interface-id: Интерфейс, на котором хост аутентифицирован.	
Описание события: Количество авторизованных пользователей на интерфейсе ниже максимального лимита пользователей в течение временного интервала. Сообщение журнала: <интерфейс-id> восстанавливается из состояния остановки обучения управления доступом на основе MAC-адресов Параметры Описание: interface-id: интерфейс, на котором аутентифицирован хост.	Предупреждение

MSTP Debug Enhancement

Описание записей журнала	**Уровень**
Описание события: Используется для записи события включения протокола Spanning Tree Protocol. Сообщение журнала: Протокол Spanning Tree включен	Информационный
Описание события: Используется для записи события, когда протокол Spanning Tree отключен. Сообщение журнала: Протокол Spanning Tree отключен	Информационный
Описание события: Используется для записи события изменения топологии экземпляра MSTP. Сообщение журнала: Topology changed (Instance : <Instance-id>,<interface_id>, MAC:<macaddr>) Параметры Описание: Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST. interface_id: Номер порта, который обнаруживает или получает информацию о топообмене. macaddr: mac-адрес системы моста.	Уведомление
Описание события: Используется для регистрации выбора нового корневого моста экземпляра MSTP. Сообщение журнала: [CIST | CIST Regional | MSTI Regional] New Root bridge selected ([Instance: <Instance-id>] MAC: <macaddr> Priority :<priority>) Параметры Описание: Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST. macaddr: mac-адрес системы моста. priority (приоритет): Значение приоритета моста должно быть кратно 4096.	Информационный
Описание события: Используется для регистрации выбора нового корневого порта экземпляра MSTP. Сообщение журнала: Выбран новый корневой порт (экземпляр:<Instance-id>, <interface_id>) Параметры Описание: Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST.	Уведомление

interface_id: Номер порта, который обнаруживает или получает информацию о topochange.	
Описание события: Используется для записи события изменения состояния порта экземпляра MSTP. Log Message: Изменение состояния порта Spanning Tree (Instance :<Instance-id>, <interface_id>) <old_status> -> <new_status>. Параметры Описание: Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST. interface_id: Номер порта, который обнаруживает или получает информацию о topochange. old status: new status: Состояние STP порта. Значение может быть Disable, Discarding, Learning, Forwarding.	Уведомление
Описание события: Используется для записи события изменения роли порта экземпляра MSTP. Log Message: Spanning Tree port role change (Instance :<Instance-id>, <interface_id>) <old_role> -> <new_role> Параметры Описание: Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST. Interface_id: Номер порта, который обнаруживает или получает информацию о топообмене. old role: new role : Роль port of stp. Значение может быть DisabledPort, AlternatePort, BackupPort, RootPort, DesignatedPort, MasterPort.	Информационный
Описание события: Используется для записи действия по созданию экземпляра MST. Log Message: Spanning Tree instance created (Instance :<Instance-id>) Parameters Description: Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST.	Информационный
Описание события: Используется для записи действия по удалению экземпляра MST. Log Message: Spanning Tree instance deleted (Instance :<Instance-id>) Parameters Description: Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST.	Информационный
Описание события: Используется для записи действия по изменению версии STP. Log Message: Изменение версии Spanning Tree (новая версия :<new_version>) Параметры Описание: new_version: Работает под какой версией STP.	Информационный
Описание события: Используется для записи измененного имени конфигурации и уровня ревизии в идентификаторе конфигурации MST.	Информационный

Сообщение журнала: Изменение имени и уровня ревизии идентификатора конфигурации MST Spanning Tree (имя: <имя>, уровень ревизии <уровень_ревизии>). Параметры Описание: name: Имя, заданное для указанного региона MST. уровень ревизии (revision_level): Коммутаторы с одинаковым именем, но с разным уровнем ревизии считаются членами разных регионов MST.	
Описание события: Используется для записи действий по сопоставлению VLAN(ов) с экземпляром MST. Сообщение журнала: Spanning Tree MST configuration ID VLAN mapping table change (instance: <Instance-id> add vlan <startvlanid> [- <endvlanid>]). Параметры Описание: Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST. startvlanid: Начальный vid диапазона add vlan. endvlanid: Конечный vid диапазона add vlan.	Информационный
Описание события: Используется для записи действия по удалению VLAN(ов) из экземпляра MST. Сообщение журнала: Изменение таблицы отображения VLAN в конфигурации MST (экземпляр: <Instance-id> delete vlan <startvlanid> [- <endvlanid>]). Параметры Описание: Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST. startvlanid: Начальный vid удаляемого диапазона vlan. endvlanid: Конечный vid удаляемого диапазона vlan.	Информационный
Описание события: Используется для записи события, когда роль порта изменилась на альтернативную из-за guard root. Log Message: Изменение роли порта Spanning Tree (Instance :<instance-id>, <interface-id>) на альтернативный порт из-за корня guard. Параметры Описание: Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST. Interface_id: Номер порта, который обнаружил событие.	Информационный

Peripheral

Описание записей журнала	**Уровень**
Описание события: Вентилятор восстановлен. Сообщение журнала: Unit <id>, <fan-descr> back to normal Параметры Описание: Unit <id>: идентификатор устройства. fan-descr: Идентификатор вентилятора и его положение.	Критический
Описание события: Отказ вентилятора. Сообщение журнала: Unit <id> <fan-descr> failed Parameters	Критический

Description: Unit <id>: идентификатор устройства. fan-descr: Идентификатор вентилятора и его положение.	
Описание события: Датчик температуры переходит в состояние тревоги. Сообщение журнала: Устройство <unit-id> <thermal-sensor-descr> обнаруживает аномальную температуру <degree>. Параметры Описание: unitID: Идентификатор устройства. thermal-sensor-descr: Идентификатор и положение датчика. градус: Текущая температура.	Критический
Описание события: Температура восстанавливается до нормы. Сообщение в журнале: Температура устройства <unit-id> <thermal-sensor-descr> вернулась к норме. Параметры Описание: unitID: идентификатор устройства. thermal-sensor-descr: Идентификатор датчика и его положение.	Критический
Описание события: Отказ питания. Log Message: Unit <unit-id> <power-descr> failed Параметры Описание: unitID: Идентификатор устройства. power-descr: Положение питания и идентификатор.	Критический
Описание события: Питание восстановлено. Log Message: Блок <unit-id> <power-descr> возвращен в нормальное состояние Параметры Описание: unitID: идентификатор устройства. power-descr: Положение и идентификатор питания.	Критический
Описание события: Нажмите кнопку сброса к заводским настройкам. Сообщение журнала: Unit <unit-id> factory reset button pressed Параметры Описание: unitID: идентификатор устройства.	Критический

PoE

Описание записей журнала	**Уровень**
Описание события: Превышен порог общего энергопотребления. Сообщение в журнале: Превышен порог использования <процент> устройства <unit-id> Параметры Описание: unit-id: идентификатор блока процент: порог использования	Предупреждение
Описание события: Восстановлен порог использования общей мощности. Сообщение в журнале: Восстановлен порог использования <процент> блока <unit-id> Параметры Описание:	Предупреждение

unit-id: идентификатор блока процент: порог использования	
Описание события: PD не отвечает на запрос ping. Сообщение журнала: PD alive check failed. (Порт: <portNum>, PD: <ipaddr>) Параметры Описание: portNum: Номер порта. ipaddr: IP-адрес (IPv4/IPv6) PD.	Предупреждение
Описание события: Отключение питания из-за отсутствия Maintain Power Signature (MPS). Log Message: ASV: Порт <port-type> <interface-id> PoE MPS Absent Параметры Описание: port-type: тип порта interface-id: имя интерфейса	Предупреждение
Описание события: Обнаружено состояние короткого замыкания. Сообщение журнала: ASV: Порт <port-type> <interface-id> PoE PD short Параметры Описание: port-type: тип порта interface-id: имя интерфейса	Предупреждение
Описание события: Обнаружено состояние перегрузки. Сообщение журнала: ASV: Порт <port-type> <interface-id> Параметры перегрузки PoE Описание: port-type: тип порта interface-id: имя интерфейса	Предупреждение
Описание события: Питание было отключено или снято из-за неисправности. Сообщение журнала: ASV: Port <port-type> <interface-id> PoE Power Denied Параметры Описание: port-type: тип порта interface-id: имя интерфейса	Предупреждение
Описание события: Питание было отключено или снято из-за перегрева. Сообщение журнала: ASV: Порт <port-type> <interface-id> PoE Thermal Shutdown Описание параметров: port-type: тип порта interface-id: имя интерфейса	Предупреждение
Описание события: Сбой запуска PoE на порту. Log Message: ASV: Port <port-type> <interface-id> PoE Startup Failure Описание параметров: port-type: тип порта interface-id: имя интерфейса	Предупреждение
Описание события: Невозможно классифицировать PD. Сообщение журнала: ASV: Port <port-type> <interface-id> PoE Classification Failure Параметры Описание: port-type: тип порта interface-id: имя интерфейса	Предупреждение

Port Security

Описание записей журнала	**Уровень**
Описание события: Заполнен адрес на порту. Сообщение журнала: MAC-адрес <macaddr> вызывает нарушение безопасности порта на <interface-id>.	Предупреждение

Параметры Описание: macaddr: MAC-адрес нарушения. interface-id: Имя интерфейса.	
Описание события: Адрес в системе заполнен. Сообщение журнала: Превышен лимит на количество записей в системе	Предупреждение

Safeguard

Описание записей журнала	**Уровень**
Описание события: хост переходит в режим истощения. Log Message: Устройство <unit-id>, Safeguard Engine переходит в режим EXHAUSTED Описание параметров: unit-id: Идентификатор устройства	Предупреждение
Описание события: хост переходит в режим нормальной работы. Log Message: Устройство <unit-id>, Safeguard Engine переходит в режим NORMAL Описание параметров: unit-id: Идентификатор устройства	Информационный

SNMP

Описание записей журнала	**Уровень**
Описание события: Получен SNMP-запрос с недопустимой строкой сообщества. Сообщение журнала: SNMP-запрос получен от <ipaddr> с недопустимой строкой сообщества. Параметры Описание: ipaddr: IP-адрес.	Информационный

SSH

Описание записей журнала	**Уровень**
Описание события: SSH-сервер включен. Сообщение журнала: SSH-сервер включен	Информационный
Описание события: SSH-сервер отключен. Сообщение журнала: SSH-сервер отключен	Информационный

Stacking

Описание записей журнала	**Уровень**
Описание события: Горячая вставка. Сообщение в журнале: Устройство: <unitID>, MAC: <macaddr> Горячая вставка Описание параметров:	Информационный

unitID: идентификатор блока. Macaddr: MAC-адрес.	
Описание события: Горячее удаление. Сообщение журнала: Устройство: <unitID>, MAC: <macaddr> Горячее удаление Параметры Описание: unitID: идентификатор блока. Macaddr: MAC-адрес.	Информационный
Описание события: Изменение топологии стекирования. Сообщение в журнале: Топология стекирования <Stack_TP_TYPE>. Master(Unit <unitID>, MAC:<macaddr>) Параметры Описание: Stack_TP_TYPE: Тип топологии стекирования является одним из следующих: 1. Ring (кольцо), 2. Chain (цепочка). UnitID: идентификатор блока. Macaddr: MAC-адрес.	Информационный
Описание события: Резервный мастер сменился ведущим. Сообщение журнала: Резервный мастер сменился мастером. Master (Unit: <unitID>) Описание параметров: UnitID: Идентификатор блока.	Информационный
Описание события: Ведомый сменился ведущим. Сообщение журнала: Ведомый сменился ведущим. Master (Unit: <unitID>) Описание параметров: UnitID: Идентификатор блока.	Информационный
Описание события: Конфликт идентификатора ящика. Сообщение журнала: Горячая вставка не удалась, конфликт идентификаторов блоков: Конфликт <unitID> блока (MAC: <macaddr> и MAC: <macaddr>). Параметры Описание: unitID: идентификатор блока. macaddr: MAC-адреса конфликтующих боксов.	Критический
Описание события: Соединение стекирующего порта. Стекирующий порт будет действовать как интерфейс SIO или член интерфейса SIO (SIO Trunk). Эта запись в журнале доступна только для проектов, у которых стекирующий порт имеет индикатор номера порта на панели устройства. Сообщение журнала: Stacking port <port> link up Параметры Описание: port: Представляет собой логический номер порта стекирующего порта.	Критический
Описание события: Отключение стекирующего порта. Стекирующий порт действует как интерфейс SIO или член интерфейса SIO (SIO Trunk). Эта запись в журнале доступна только для проектов, у которых стекирующий порт имеет индикатор номера порта на панели устройства. Сообщение журнала: Stacking port <port> link down Параметры Описание:	Критический

port: Представляет собой логический номер порта стекирующего порта.	
Описание события: Подключение интерфейса SIO. Для SIO Trunk это событие возникает при подключении первого порта-члена. Log Message: SIO interface Unit <unitID> <SIOn> link up Параметры Описание: unitID: идентификатор блока. SIOn: Представляет номер интерфейса SIO. Текущий поддерживаемый номер интерфейса SIO должен быть SIO1 и SIO2.	Критический
Описание события: Отключение соединения интерфейса SIO. Для SIO Trunk это событие инициируется при отключении связи последнего порта-члена. Log Message: SIO interface Unit <unitID> <SIOn> link down Параметры Описание: UnitID: Идентификатор блока. SIOn: Представляет номер интерфейса SIO. Текущий поддерживаемый номер интерфейса SIO должен быть SIO1 и SIO2.	Критический

Storm Control

Описание записей журнала	**Уровень**
Описание события: Возникновение шторма. Log Message: <Broadcast | Multicast | Unicast> storm is occurring on <interface-id>. Параметры Описание: Broadcast: Шторм вызван широковещательными пакетами (DA = FF:FF:FF:FF:FF:FF:FF:FF). Multicast: Шторм вызван многоадресными пакетами, включая неизвестные L2 multicast, известные L2 multicast, неизвестные IP multicast и известные IP multicast. Одноадресная передача: Шторм вызван одноадресными пакетами, включая известные и неизвестные одноадресные пакеты. interface-id: Идентификатор интерфейса, на котором происходит шторм.	Предупреждение
Описание события: Шторм устранен. Log Message: <Broadcast | Multicast | Unicast> шторм очищен на <interface-id>. Описание параметров: Broadcast: Широковещательный шторм устранен. Multicast: Многоадресный шторм очищен. Одноадресная передача: Одноадресный шторм (включая как известные, так и неизвестные одноадресные пакеты) очищен. interface-id: Идентификатор интерфейса, на котором очищается шторм.	Информационный
Описание события: Порт отключен из-за пакетного шторма.	Предупреждение

Сообщение журнала: <Интерфейс-id> в настоящее время отключен из-за шторма <Broadcast | Multicast | Unicast>. Параметры Описание: interface-id: Идентификатор интерфейса, на котором произошла ошибка отключения из-за шторма. Broadcast: Интерфейс отключен широковещательным штормом. Multicast: Интерфейс отключен многоадресным штормом. Unicast: Интерфейс отключен одноадресным штормом (включая как известные, так и неизвестные одноадресные пакеты).	

System Log Summary

Описание записей журнала	**Уровень**
Описание события: Этот журнал будет создан при теплом запуске системы. Сообщение журнала: [Unit <unitID>,]теплый запуск системы Параметры Описание: unitID: идентификатор устройства.	Критический
Описание события: Этот журнал генерируется при холодном запуске системы. Сообщение журнала: [Unit <unitID>,]холодный запуск системы Параметры Описание: unitID: идентификатор устройства.	Критический
Описание события: Этот журнал генерируется при запуске системы. Сообщение журнала: [Unit <unitID>,]Система запущена. Параметры Описание: unitID: идентификатор устройства.	Критический

Telnet

Описание записей журнала	**Уровень**
Описание события: Успешный вход в систему через Telnet. Сообщение в журнале: Успешный вход в систему через Telnet (имя пользователя: <username>, IP: <ipaddr>) Параметры Описание: ipaddr: IP-адрес клиента telnet. username: имя пользователя, которое используется для входа на сервер telnet.	Информационный
Описание события: Не удалось войти в систему через Telnet. Сообщение журнала: Не удалось войти в систему через Telnet (имя пользователя: <username>, IP: <ipaddr>). Параметры Описание: ipaddr: IP-адрес клиента telnet. username: имя пользователя, которое используется для входа на сервер telnet.	Предупреждение

Описание события: Выход из системы через Telnet. Сообщение журнала: Выход из системы через Telnet (Имя пользователя: <username>, IP: <ipaddr>) Параметры Описание: ipaddr: IP-адрес клиента telnet. username: имя пользователя, которое используется для входа на сервер telnet.	Информационный
Описание события: Сессия Telnet завершилась по таймеру. Сообщение журнала: Сессия Telnet завершилась (имя пользователя: <username>, IP: <ipaddr>). Параметры Описание: ipaddr: IP-адрес клиента telnet. username: имя пользователя, используемое для входа на сервер telnet.	Информационный

Voice-VLAN

Описание записей журнала	**Уровень**
Описание события: При обнаружении нового голосового устройства на интерфейсе. Сообщение журнала: Обнаружено новое голосовое устройство (<interface-id>, MAC: <mac-адрес>) Параметры Описание: interface-id: Имя интерфейса. mac-адрес: MAC-адрес голосового устройства	Информационный
Описание события: Когда интерфейс, находящийся в режиме автоматической голосовой VLAN, присоединяется к голосовой VLAN. Log Message: <interface-id> add into voice VLAN <vid> Параметры Описание: interface-id: Имя интерфейса. vid:ID VLAN	Информационный
Описание события: Когда интерфейс покидает голосовую VLAN и в то же время в интервале старения для этого интерфейса не обнаружено голосовое устройство, будет отправлено сообщение журнала. Сообщение журнала: <interface-id> remove from voice VLAN <vid> Описание параметров: interface-id: Имя интерфейса. vid:Идентификатор виртуальной локальной сети.	Информационный

Web

Описание записей журнала	**Уровень**
Описание события: Успешный вход в систему через Web. Сообщение журнала: Успешный вход в систему через Web (имя пользователя: <username>, IP: <ipaddr>) Описание параметров: username: Имя пользователя, используемое для входа на	Информационный

HTTP-сервер. ipaddr: IP-адрес HTTP-клиента.	
Описание события: Не удалось войти в систему через Web. Сообщение журнала: Не удалось войти в систему через Web (имя пользователя: <username>, IP: <ipaddr>). Параметры Описание: username: Имя пользователя, используемое для входа на HTTP-сервер. ipaddr: IP-адрес HTTP-клиента.	Предупреждение
Описание события: Выход из системы через веб. Сообщение журнала: Logout through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: Имя пользователя, используемое для входа на HTTP-сервер. ipaddr: IP-адрес HTTP-клиента.	Информационный
Описание события: Успешный вход в систему через Web (SSL). Сообщение в журнале: Успешный вход в систему через Web (SSL) (имя пользователя: <username>, IP: <ipaddr>). Описание параметров: username: Имя пользователя, используемое для входа на сервер SSL. ipaddr: IP-адрес клиента SSL.	Информационный
Описание события: Не удалось войти в систему через Web (SSL). Сообщение в журнале: Не удалось войти в систему через Web (SSL) (имя пользователя: <username>, IP: <ipaddr>). Параметры Описание: username: Имя пользователя, используемое для входа на сервер SSL. ipaddr: IP-адрес клиента SSL.	Предупреждение
Описание события: Веб-сессия (SSL) завершилась по таймеру. Сообщение в журнале: Веб-сессия (SSL) завершилась (имя пользователя: <username>, IP: <ipaddr>). Параметры Описание: имя пользователя: имя пользователя, используемое для входа на сервер SSL. ipaddr: IP-адрес клиента SSL.	Информационный
Описание события: Выход из системы через Web(SSL). Сообщение журнала: Выход из системы через Web(SSL) (Имя пользователя: <username>, IP: <ipaddr>). Параметры Описание: username: Имя пользователя, используемое для входа на сервер SSL. ipaddr: IP-адрес клиента SSL.	Информационный

Web-Authentication

Описание записей журнала	**Уровень**
Описание события: Когда хост прошел проверку подлинности. Сообщение журнала: Web-Authentication host login success (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <mac-адрес>, <interface-id>, VID: <vlan- id>) Параметры Описание: Имя пользователя: Имя пользователя хоста.	Информационный

IP: IP-адрес хоста mac-адрес: MAC-адреса хоста. interface-id: Интерфейс, на котором хост аутентифицирован. vlan-id: Идентификатор виртуальной локальной сети, в которой существует хост.	
Описание события: Когда хост не проходит аутентификацию. Сообщение журнала: Web-Authentication host login fail (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <mac-адрес>, <interface-id>, VID: <vlan-id>) Параметры Описание: Имя пользователя: Имя пользователя хоста. IP: IP-адрес хоста. mac-адрес: MAC-адрес хоста. interface-id: Интерфейс, на котором хост аутентифицирован. vlan-id: Идентификатор виртуальной локальной сети, в которой существует хост.	Критический
Описание события: когда количество авторизованных пользователей на всем устройстве достигло максимального предела. Сообщение журнала: Web-аутентификация вошла в состояние остановки обучения	Предупреждение
Описание события: когда количество авторизованных пользователей на всем устройстве ниже максимального предела пользователей в течение определенного интервала времени. Сообщение журнала: Web-аутентификация восстанавливается из состояния остановки обучения	Предупреждение

Приложение Б. Записи trap-сообщений

В следующей таблице перечислены все возможные записи trap-сообщений и их соответствующие значения, которые появятся в коммутаторе.

802.1X

Сообщение trap	Описание	OID
dDot1xExtLoggedSuccess	Хост прошел аутентификацию 802.1X. Вариабельные привязки: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName	1.3.6.1.4.1.17 1.14.30.0.1
dDot1xExtLoggedFail	Хост не прошел аутентификацию 802.1X.	1.3.6.1.4.1.17 1.14.30.0.2

	Вариабельные привязки: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName (5) dDot1xExtNotifyFailReason

Authentication Fail

Сообщение trap	Описание	OID
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

BPDU Protection

Сообщение trap	Описание	OID
dBpduProtectionAttackOccur	Атака BPDU на интерфейсе. Вариабельные привязки: (1) ifIndex (2) dBpduProtectionIfCfgMode	1.3.6.1.4.1.17 1.14.47.0.1
dBpduProtectionAttackRecover	Атака BPDU на интерфейсе устранена. Вариабельные привязки: (1) ifIndex	1.3.6.1.4.1.17 1.14.47.0.2

DDM

Сообщение trap	Описание	OID
dDdmAlarmTrap	Возникновение проблем уровня alarm или возвращение к нормальному состоянию после устранения данных проблем. Trap-сообщение об устранении проблем будет отправлено, если текущее значение выше заданного нижнего порога alarm или ниже заданного верхнего порога alarm. Вариабельные привязки: (1) dDdmNotifyInfoIfIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.17 1.14.72.0.1

dDdmWarningTrap	Возникновение проблем уровня warning или возвращение к нормальному состоянию после устранения данных проблем. Вариабельные привязки: (1) dDdmNotifyInfoIfIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.17 1.14.72.0.2

DHCP Server Screen Prevention

Сообщение trap	Описание	OID
dDhcpFilterAttackDetected	Если функция DHCP Server Screen включена, trap-сообщения будут отправлены при получении каждого пакета 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
dDosPreveAttackDetectedPacket	Обнаружена DoS-атака. Вариабельные привязки: (1) dDoSPrevCtrlAttackType (2) dDosPrevNotiInfoDropIpAddr (3) dDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.17 1.14.59.0.2

ErrDisable

Сообщение trap	Описание	OID
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
dErrDisNotifyPortDisabledClear	Порт возвращается в исходное состояние по истечению 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
dGenMgmtLoginFail	Эта ловушка отправляется при неудачном входе пользователя в систему коммутатора. Объекты привязки: (1) dGenMgmtNotifyInfoLoginType (2) dGenMgmtNotifyInfoUserName	1.3.6.1.4.1.17 1.14.165.0.1

Gratuitous ARP

Сообщение trap	Описание	OID
agentGratuitousARPTrap	Обнаружен конфликт IP-адреса. Вариабельные привязки: (1) ipaddr (2) macaddr (3) portNumber (4) agentGratuitousARPInterfaceName	1.3.6.1.4.1.17 1.14.45.0.1

IMPB

Сообщение trap	Описание	OID
dImpbViolationTrap	Уведомление о нарушении адреса генерируется при обнаружении нарушения адреса привязки IP-MAC-Port. Объекты привязки: (1) ifIndex (2) dImpbViolationIpAddrType (3) dImpbViolationIpAddress (4) dImpbViolationMacAddress	1.3.6.1.4.1.17 1.14.22.0.1

LACP

Сообщение trap	Описание	OID
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
linkDown	SNMP-устройство в роли агента	1.3.6.1.6.3.1.1

	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	.5.3

LBD

Сообщение trap	Описание	OID
swPortLoopOccurred	Обнаружена петля. Вариабельные привязки: (1) swLoopDetectPortIndex	1.3.6.1.4.1.17 1.14.46.0.1
swPortLoopRestart	Порт возвращается в исходное состояние по истечению определенного интервала времени. Вариабельные привязки: (1) swLoopDetectPortIndex	1.3.6.1.4.1.17 1.14.46.0.2
swVlanLoopOccurred	Обнаружена петля в режиме LBD VLAN-Based. Вариабельные привязки: (1) swLoopDetectPortIndex (2) swVlanLoopDetectVID	1.3.6.1.4.1.17 1.14.46.0.3
swVlanLoopRestart	Порт возвращается в исходное состояние в режиме LBD VLAN-based по истечению определенного интервала времени. Вариабельные привязки: (1) swLoopDetectPortIndex (2) swVlanLoopDetectVID	1.3.6.1.4.1.17 1.14.46.0.4

LLDP-MED

Сообщение trap	Описание	OID
lldpRemTablesChange	Значение lldpStatsRemTableLastChangeTime изменилось. Вариабельные привязки: (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.0.8802.1.1.2 .0.0.1
lldpXMedTopologyChangeDetected	Обнаружено изменение в топологии: к порту было подключено новое устройство, удаленное устройство было отключено или было отключено с дальнейшем	1.0.8808.1.1.2 .1.5.4795.0.1

	подключением к другому порту. Вариабельные привязки: (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass	

MAC-based Access Control

Сообщение trap	Описание	OID
dMacAuthLoggedSuccess	Хост успешно прошел аутентификацию на основе MAC. Вариабельные привязки: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.17 1.14.153.0.1
dMacAuthLoggedFai	Хост не прошел аутентификацию на основе MAC. Вариабельные привязки: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.17 1.14.153.0.2
dMacAuthLoggedAgesOut	Время аутентификации хоста истекло. (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.17 1.14.153.0.3

MAC Notification

Сообщение trap	Описание	OID
dL2FdbMacNotification	Изменение MAC-адресов в таблице коммутации. Вариабельные привязки: (1) dL2FdbMac ChangeNotifyInfo	1.3.6.1.4.1.17 1.14.3.0.1

MSTP

Сообщение trap	Описание	OID
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
topologyChange	Мост отправляет trap-собщение, когда какой-то из его настроенных портов	1.3.6.1.2.1.17. 0.2

	переходит из состояния Learning в состояние Forwarding или из состояния Forwarding в состояние Blocking. Данное trap-сообщение не отправляется повторно. Отправка данного trap-сообщения является опциональной.	

Peripheral

Сообщение trap	Описание	OID
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 (2) dEntityExtEnvFanIndex (3) dEntityExtEnvFanStatus	1.3.6.1.4.1.17 1.14.5.0.1
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
dEntityExtPowerStatusChg	Выход из строя, удаление или восстановление модуля питания. Данное trap-сообщение отправляется Commander Switch. Вариабельные привязки: (1) dEntityExtEnvPowerUnitId (2) dEntityExtEnvPowerIndex (3) dEntityExtEnvPowerStatus	1.3.6.1.4.1.17 1.14.5.0.3
dEntityExtFactoryResetButton	Нажмите кнопку сброса к заводским настройкам. Объекты привязки: (1) dEntityExtUnitIndex	1.3.6.1.4.1.17 1.14.5.0.5

PoE

Сообщение trap	**Описание**	**OID**
pethMainPowerUsageOnNotification	Эта ловушка указывает на включение индикации использования PSE Threshold, мощность использования выше порога. Между уведомлениями, испускаемыми одним и тем же экземпляром объекта, должно пройти не менее 500 мс. Связывающие объекты: (1) pethMainPseConsumptionPower	1.3.6.1.2.1.10 5.0.2
pethMainPowerUsageOffNotification	Эта ловушка указывает на то, что индикация использования PSE Threshold выключена, мощность использования ниже порогового значения. Между уведомлениями, испускаемыми одним и тем же экземпляром объекта, должно пройти не менее 500 мс. Связывающие объекты: (1) pethMainPseConsumptionPower	1.3.6.1.2.1.10 5.0.3
dPoeIfPowerDeniedNotification	Это уведомление указывает, если диаграмма состояния PSE переходит в состояние POWER_DENIED. Между уведомлениями, испускаемыми одним и тем же экземпляром объекта, должно пройти не менее 500 мс. Связывающие объекты: (1) pethPsePortPowerDeniedCounter	1.3.6.1.4.1.17 1.14.24.0.1
dPoeIfPowerOverLoadNotification	Эта ловушка указывает, если диаграмма состояния PSE переходит в состояние ERROR_DELAY_OVER. Между уведомлениями, испускаемыми одним и тем же экземпляром объекта, должно пройти не менее 500 мс. Связывающие объекты: (1) pethPsePortOverLoadCounter	1.3.6.1.4.1.17 1.14.24.0.2
dPoeIfPowerShortCircuitNotification	Эта ловушка указывает, если диаграмма состояния PSE переходит в состояние ERROR_DELAY_SHORT. Между уведомлениями, испускаемыми одним и тем же экземпляром объекта, должно пройти не менее 500 мс. Связывающие объекты: (1) pethPsePortShortCounter	1.3.6.1.4.1.17 1.14.24.0.3
dPoeIfPdAliveFailOccurNotification	Этот трап указывает на то, что устройство PD перестало работать или не отвечает. Между уведомлениями, испускаемыми одним и тем же экземпляром объекта, должно пройти не менее 500 мс. Связывающие объекты: (1) pethMainPseGroupIndex (2) pethPsePortIndex	1.3.6.1.4.1.17 1.14.24.0.4

	(3) dPoeIfPdAliveCfgPdIpType (4) dPoeIfPdAliveCfgPdIpAddr

Port

Сообщение trap	Описание	OID
linkUp	При соединении портов генерируется уведомление. Объекты привязки: (1) ifIndex (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1. 1.5.4
linkDown	При отключении порта генерируется уведомление. Объекты привязки: (1) ifIndex (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1. 1.5.3

Port Security

Сообщение trap	Описание	OID
dPortSecMacAddrViolation	Если отправка trap-сообщений Port Security включена, 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
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
fallingAlarm	Запись уровня alarm снизилась до заданного нижнего порога. Вариабельные привязки: (1) alarmIndex (2) alarmVariable (3) alarmSampleType	1.3.6.1.2.1.16. 0.2

	(4) alarmValue (5) alarmFallingThreshold

Safeguard

Сообщение trap	Описание	OID
dSafeguardChgToExhausted	Нормальный режим работы системы изменился на режим высокой загрузки. Вариабельные привязки: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.17 1.14.19.1.1.0. 1
dSafeguardChgToNormal	Режим высокой загрузки системы изменился на нормальный режим. Вариабельные привязки: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.17 1.14.19.1.1.0. 2

Stack

Сообщение trap	Описание	OID
dStackInsertNotification	«Горячее» добавление модуля. Вариабельные привязки: (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.17 1.14.9.0.1
dStackRemoveNotification	«Горячее» удаление модуля. Вариабельные привязки: (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.17 1.14.9.0.2
dStackFailureNotification	Ошибка подключения модуля. Вариабельные привязки: (1) dStackNotifyInfoBoxId	1.3.6.1.4.1.17 1.14.9.0.3
dStackTPChangeNotification	Изменение топологии стекирования. Вариабельные привязки: (1) dStackNotifyInfoTopologyType (2) dStackNotifyInfoBoxId (3) dStackInfoMacAddr	1.3.6.1.4.1.17 1.14.9.0.4
dStackRoleChangeNotification	Изменение роли модуля в стеке. Вариабельные привязки: (1) dStackNotifyInfoRoleChangeType (2) dStackNotifyInfoBoxId	1.3.6.1.4.1.17 1.14.9.0.5

SIM

Сообщение trap	Описание	OID
swSingleIPMSColdStart	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление о «холодном» старте.	1.3.6.1.4.1.17 1.12.8.6.0.11

	Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	
swSingleIPMSWarmStart	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление о «горячем» старте. Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.12
swSingleIPMSLinkDown	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление о прерванном соединении. Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.17 1.12.8.6.0.13
swSingleIPMSLinkUp	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление об установленном соединении. Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.17 1.12.8.6.0.14
swSingleIPMSAuthFail	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление об ошибки аутентификации. Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.15
swSingleIPMSnewRoot	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление о новом корне. Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.16
swSingleIPMSTopologyChange	Данное trap-сообщений будет	1.3.6.1.4.1.17

	отправлено Commander Switch, если участником его группы было сгенерировано уведомление об изменении топологии. Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.12.8.6.0.17

Start

Сообщение trap	Описание	OID
coldStart	Повторная инициализация SNMPv2-устройства в роли агента и возможное изменение его настроек.	1.3.6.1.6.3.1.1 .5.1
warmStart	Повторная инициализация SNMPv2-устройства в роли агента с неизмененной конфигурацией.	1.3.6.1.4.1.17 1.14.9.0.2

System File

Сообщение trap	Описание	OID
dsfUploadImage	Пользователь успешно выгрузил файл образа.	1.3.6.1.4.1.17 1.14.14.0.1
dsfDownloadImage	Пользователь успешно загрузил файл образа.	1.3.6.1.4.1.17 1.14.14.0.2
dsfUploadCfg	Пользователь успешно выгрузил конфигурационный файл.	1.3.6.1.4.1.17 1.14.14.0.3
dsfDownloadCfg	Пользователь успешно загрузил конфигурационный файл.	1.3.6.1.4.1.17 1.14.14.0.4
dsfSaveCfg	Пользователь успешно сохранил конфигурационный файл.	1.3.6.1.4.1.17 1.14.14.0.5

Web-Authentication

Сообщение trap	Описание	OID
dWebAuthLoggedSuccess	Ловушка отправляется, когда хост успешно вошел в систему (прошел Web-аутентификацию). Объекты привязки: (1) ifIndex (2) dnaSessionAuthVlan (3) dnaSessionClientMacAddress (4) dnaSessionClientAddrType (5) dnaSessionClientAddress (6) dnaSessionAuthUserName	1.3.6.1.4.1.17 1.14.154.0.1
dWebAuthLoggedFail	Ловушка отправляется, когда хост не смог пройти Web-аутентификацию (вход	1.3.6.1.4.1.17 1.14.154.0.2

	не удался). Объекты привязки: (1) ifIndex (2) dnaSessionAuthVlan (3) dnaSessionClientMacAddress (4) dnaSessionClientAddrType (5) dnaSessionClientAddress (6) dnaSessionAuthUserName

Приложение B - Назначение атрибутов RADIUS

Назначение атрибутов RADIUS на ТГК-151 используется в следующих модулях: Console, Telnet, SSH, Web, 802.1X, контроль доступа на основе MAC, JWAC и WAC.

Следующее описание объясняет следующие типы назначений атрибутов RADIUS:

- Privilege Level
- Ingress/Egress Bandwidth
- 802.1p Default Priority
- VLAN
- ACL

Для того, чтобы RADIUS-сервер назначил **уровень привилегии**, необходимо сконфигурировать соответствующие параметры на сервере. В таблице ниже приведены параметры для полосы пропускания.

Параметрами атрибутов Vendor-Specific являются:

Атрибут для производителя	**Описание**	**Значение**	**Использование**
Vendor-ID	Определяет производителя	171 (DLINK)	Обязательно
Vendor-Type	Определяет атрибут	1	Обязательно
Attribute-Specific Field	Используется для назначения уровня привилегии пользователя для работы с коммутатором	Диапазон (1-15)	Обязательно

Если пользователь настроил атрибут уровня привилегий сервера RADIUS (например, уровень 15) и аутентификация Console, Telnet, SSH и Web прошла успешно, устройство назначит уровень привилегий (согласно данным сервера RADIUS) этому пользователю доступа. Однако, если пользователь не настроил атрибут уровня привилегий и успешно прошел аутентификацию, устройство не будет назначать уровень привилегий пользователю доступа. Если уровень привилегий настроен меньше минимального поддерживаемого значения или больше максимального поддерживаемого значения, уровень привилегий будет проигнорирован.

Для того, чтобы RADIUS-сервер назначил **входящую/исходящую полосу пропускания**, необходимо сконфигурировать соответствующие параметры на сервере. В таблице ниже приведены параметры для полосы пропускания.

Параметрами атрибутов Vendor-Specific являются:

Атрибут для производителя	**Описание**	**Значение**	**Использование**
Vendor-ID	Определяет производителя	171 (DLINK)	Обязательно
Vendor-Type	Определяет атрибут	2 (для входящей полосы) 3 (для исходящей	Обязательно

		полосы)	
Attribute-Specific Field	Используется для назначения полосы пропускания порта	Unit (Kbits)	Обязательно

Если пользователь настроил атрибут полосы пропускания сервера RADIUS (например, ingress bandwidth 1000Kbps), и аутентификация 802.1X, MAC-based Access Control, JWAC или WAC прошла успешно, устройство назначит порту полосу пропускания (согласно данным сервера RADIUS). Однако, если пользователь не настроил атрибут полосы пропускания и успешно прошел аутентификацию, устройство не будет назначать порту никакой полосы пропускания. Если атрибут полосы пропускания настроен на сервере RADIUS со значением "0", эффективная полоса пропускания будет установлена "no_limited", а если полоса пропускания настроена меньше "0" или больше максимально поддерживаемого значения, полоса пропускания будет проигнорирована.

Для того, чтобы RADIUS-сервер назначил **приоритет по умолчанию 802.1p**, необходимо сконфигурировать соответствующие параметры на сервере. В таблице ниже приведены параметры для приоритета 802.1p.

Параметрами атрибутов Vendor-Specific являются:

Атрибут для производителя	**Описание**	**Значение**	**Использование**
Vendor-ID	Определяет производителя	171 (DLINK)	Обязательно
Vendor-Type	Определяет атрибут	4	Обязательно
Attribute-Specific Field	Используется для назначения приоритета по умолчанию 802.1p порта	0-7	Обязательно

Если пользователь настроил атрибут приоритета 802.1p на сервере RADIUS (например, приоритет 7) и аутентификация по 802.1X, MAC-based Access Control, JWAC или WAC прошла успешно, устройство назначит порту приоритет 802.1p по умолчанию (согласно данным сервера RADIUS). Однако, если пользователь не настроил атрибут приоритета и успешно прошел аутентификацию, устройство не будет назначать приоритет этому порту. Если атрибут приоритета, настроенный на сервере RADIUS, имеет значение вне диапазона (>7), он не будет установлен устройством.

Для того, чтобы RADIUS-сервер назначил **VLAN**, необходимо сконфигурировать соответствующие параметры на сервере. Для назначения VLAN RFC 3580 определяет следующие атрибуты в пакетах RADIUS.

В таблице ниже приведены 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 транспортную	6 (802)	Обязательно

	Среду.		
Tunnel-Private-Group-ID	Атрибут указывает групповой ID для определенной туннельной сессии.	string	Обязательно

Краткое описание формата атрибута Tunnel-Private-Group-ID показано ниже.

В таблице ниже приведено определение поля Tag (отличается от RFC 2868):

Значение поля Tag	**Формат строки поля**
0x01	Имя 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, WAC или на основе MAC прошла успешно, порт будет назначен VLAN 3. Однако если пользователь не сконфигурировал атрибуты VLAN, порт, который не является членом Guest VLAN, будет храниться в текущей аутентификации VLAN, а порт, являющийся членом Guest VLAN, будет назначен в исходную VLAN.

Для того, чтобы RADIUS-сервер назначил **ACL**, необходимо сконфигурировать соответствующие параметры на сервере. В таблице ниже приведены параметры для ACL.

- **VSA14 ACL Script**

Параметрами атрибута Vendor-Specific Attribute являются:

Атрибут для производителя	**Описание**	**Значение**	**Использование**
Vendor-ID	Определяет производителя	171 (DLINK)	Обязательно
Vendor-Type	Определяет атрибут	14 (для ACL Script)	Обязательно
Attribute-Specific Field	Используется для назначения ACL Script. Формат основывается на	ACL Script Например: **ip access-list**	Обязательно

	командах списка управления доступом (ACL)	**a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;**

Если пользователь настроил атрибут ACL на сервере RADIUS (например, сценарий ACL: ip access- list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;), и WAC 802.1X или MAC-based Access Control успешно работает, устройство назначит сценарий ACL в соответствии с сервером RADIUS. Параметры входа в **Access-List Configuration Mode** и выхода из **Access-List Configuration Mode** должны быть парой, иначе сценарий ACP будет отклонен. Для получения дополнительной информации о модуле ACL обратитесь к главе Команды списка контроля доступа (ACL).

- **NAS-Filter-Rule (92)**

В таблице ниже приведены параметры для NAS-Filter-Rule:

Атрибут туннеля RADIUS	**Описание**	**Значение**	**Использование**
NAS-Filter-Rule	Этот атрибут указывает правила фильтрации, которые будут применяться к пользователю.	Строка (объединяющая отдельные правила фильтрации, разделенные октетом NUL (0x00))	Обязательно

Filter Rule Format

Используйте команду **permit** для добавления разрешающей записи. Используйте команду **deny** для добавления запрещающей записи.

{permit | deny} in tcp from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR***} [***TCP-PORT-RANGE***]**

{permit | deny} in udp from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6- ADDR* **|** *DST-IPV6-NET-ADDR***} [***UDP-PORT-RANGE***]**

{permit | deny} in icmp from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6- ADDR* **|** *DST-IPV6-NET-ADDR***} [***ICMP-TYPE***]**

{permit | deny} in ip from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR***}**

{permit | deny} in *IP-PROT-VALUE* **from any to {any |** *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR***}**

Параметры

in	Указывает входящий трафик.
any	Указывает любой IP-адрес источника или любой IP-адрес назначения для настройки.
DST-IP-ADDR	Указывает конкретный IP-адрес узла назначения.
DST-IP-NET-ADDR	Указывает группу IP-адресов назначения с шириной маски вида 1.2.3.4/24.

DST-IPV6-ADDR	Указывает конкретный IPv6-адрес узла назначения.
ST-IPV6-NET-ADDR	Указывает группу сети IPv6 назначения вида 2000::1/64.
TCP-PORT-RANGE	(Опционально) Указывает соответствие порту TCP или диапазону портов. Форма выглядит следующим образом: 22-23, 80.
tcp, udp, icmp	Определяет протоколы уровня 4.
ip	Указывает, что будет соответствовать любой протокол.
IP-PROT-VALUE	Указывает значение протокола IP. Допустимое значение - от 0 до 255.
UDP-PORT-RANGE	(Опционально) Указывает соответствие порта UDP или диапазона портов. Форма выглядит следующим образом: 56, 67-68.
ICMP-TYPE	(Опционально) Указывает тип сообщения ICMP. Допустимое число для типа сообщения - от 0 до 255.

Пример

В этом примере показано, как запретить службу telnet хоста на сервере RADIUS.

```
Nas-filter-Rule="deny in tcp from any to any 23"
Nas-filter-Rule+="permit in ip from any to any"
```

В этом примере показано, как ограничить доступ хоста к группе IP-адресов на сервере RADIUS.

```
Nas-filter-Rule="permit in ip from any to 10.10.10.1/24"
Nas-filter-Rule+="permit in ip from any to fe80::d1:1/64"
```

Параметрами атрибута Vendor-Specific Attribute являются:

Атрибут для производителя	**Описание**	**Значение**	**Использование**
Vendor-ID	Определяет производителя.	171 (DLINK)	Обязательно
Vendor-Type	Определяет атрибут.	14 (for ACL script)	Обязательно
Attribute-Specific Field	Правило фильтрации IPv6, используется для приема входных данных, связанных с адресами IPv6.	Этот атрибут указывает на один из следующих режимов IP для NAS-фильтра-правила 1=Передача трафика IPv4 и IPv6 2=Передавать только IPv4 трафик (отбрасывать любой IPv6 трафик). Если этот атрибут не назначен	Обязательно

	сервером RADIUS, пересылается только трафик IPv4, любой пакет IPv6 будет отброшен.

Примечание: Если одновременно назначены собственный сценарий ACL (VSA14) и стандартное NAS-Filter-Rule (92), NAS-Filter-Rule (92) вступит в силу, а VSA14 будет проигнорировано.

Приложение Г - Поддержка атрибутов IETF RADIUS

Для атрибутов RADIUS существуют определенные детали 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 вендорам создавать собственные дополнительные атрибуты RADIUS. Для подробной информации о VSA D-Link обратитесь к **Приложению Г, «Назначение атрибутов RADIUS».**

Атрибуты RADIUS стандарта IETF определены в RFC 2865 Remote Authentication Dial-In User Service (RADIUS), RFC 2866 RADIUS Accounting, RFC 2868 RADIUS Attributes for Tunnel Protocol Support и RFC 2869 RADIUS Extensions.

Список атрибутов IETF RADIUS, поддерживаемых коммутатором T-KOM, 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

Атрибуты RADIUS Accounting:

Номер	**Атрибут IETF**
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
8	Framed-IP-Address
31	Calling-Station-ID
32	NAS-Identifier
40	Acct-Status-Type
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-ID
45	Acct-Authentic
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
52	Acct-Input-Gigawords
53	Acct-Output-Gigawords
61	NAS-Port-Type
95	NAS-IPv6-Address

Приложение Д - Информация об ERPS

Только аппаратный ERPS (внешний PHY) поддерживает функцию прерывания быстрого разрыва соединения с временем восстановления 50 мс.

Название модели	ERPS	Порт 1 - 20
ТГК-151-16/4д-М	Hardware-based	
ТГК-151-16/4д-М	Software-based	V

Название модели	ERPS	Порт 1 - 8	Порт 9-28
ТГК-151-24/4д	Hardware-based	V	
ТГК-151-24/4Д-П ТГК-151-24/4д-М ТГК-151-24/4Д-2П	Software-based		V

Название модели	ERPS	Порт 1 - 8	Порт 9-24	Порт 25-32	Порт 33-52
ТГК-151-24/4д	Hardware-based	V		V	
	Software-based		V		V

Название модели	ERPS	Порт 1 - 16	Порт 17-24	Порт 25-40	Порт 41-48	Порт 49-52
ТГК-151-48/4д-М ТГК-151-48/4д-2П	Hardware-based		V		V	
ТГК-151-48/4д-М ТГК-151-48/4д-2П	Software-based	V		V		V