Руководство пользователя (CLI)

Серия DXS-1210

Настраиваемые 10-гигабитные коммутаторы уровня 2+

Версия 1.00

Содержание

1. Введение

Описания команд в данном руководстве основаны на программном обеспечении версии 2.00.008. Перечисленный здесь список команд является подгруппой команд, поддерживаемых настраиваемыми коммутаторами серии DXS-1210.

Аудитория

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

Условные обозначения

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

Предупреждения

При использовании данного руководства для управления коммутатором обращайте внимание на следующие 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.

Описания команд

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

- **Описание** – краткое описание функционала команды.
- **Синтаксис** – точная форма команды и правила ее написания.
- **Параметры** – таблица с кратким описанием необязательных или обязательных для ввода параметров и их использованием в команде.
- **По умолчанию** – если команда задает новое значение конфигурации или административное состояние коммутатора, которые отличаются от настроек по умолчанию, то это указывается в данном поле.
- **Режим ввода команды** – режим, в котором возможно использование команды. Режимы описаны в разделе «Режимы ввода команд».
- **Уровень команды по умолчанию** – уровень привилегий 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-й уровень привилегии. Данный уровень учетной записи обладает самым

низким приоритетом среди учетных записей и позволяет пользователю получить доступ к просмотру базовой информации о системе.

- **Operator** – 12-й 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-й 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 привилегий **Basic user** осуществляют вход в режиме **User EXEC Mode.**
- Пользователи с расширенным уровнем доступа: **Operator** или **Administrator**, осуществляют 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 /	Самый низкий уровень приоритета среди

Уровень Basic User	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.

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.

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-1210-16TC 10 Gigabit Ethernet Switch

                             Command Line Interface
                            Firmware: Build V2.00.007
          Copyright(C) 2021 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:

- Unit ID / Slot ID / ID порта

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. При выключении 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.

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 V2.00.007
#         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 V2.00.007
#         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 V2.00.007
#         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 Page ENTER Next Entry a All
```

2. Базовые команды интерфейса командной строки

2.1. help

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

help

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

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
```

Следующий пример показывает использование справки **по синтаксису команды**, позволяющей получить недостающий аргумент для частично введенной команды **IP access-list standard**. Символы, введенные перед вопросительным знаком (?), также отображаются на следующей строке, что позволяет пользователю продолжить ввод команды.

```
Switch(config)#ip access-list standard ?
<1-1999>            Standard IP access-list number
<cr>

Switch(config)#ip access-list standard
```

2.2. configure terminal

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

configure terminal

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User EXEC Mode

Privilege EXEC Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для входа в режим глобальной конфигурации.

Пример

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

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

2.3. logout

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

logout

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User EXEC Mode

Privilege 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 показано, как выйти из системы.

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

2.4. 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 конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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

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

2.5. 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

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.

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)#
```

2.6. 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
Любой режим конфигурирования

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#
```

2.7. show environment

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

show environment [fan | temperature]

Параметры

fan	(Опционально) Укажите, чтобы отобразить детальную информацию о состоянии вентиляторов.
temperature	(Опционально) Укажите, чтобы отобразить детальную информацию о температуре.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если тип не указан, отображаться будут все типы информации.

Пример

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

```
Switch# show environment

Detail Temperature Status:
Temperature Descr/ID   Current/Threshold Range   Temper Status
--------------------   -----------------------   -------------
Central Temperature/1  38/10~70                  in threshold range

Detail Fan Status:
----------------------------------------
  Right Fan1: Ok-Low
  Right Fan2: Ok-Low
  Right Fan3: Ok-Low
```

2.8. show unit

Данная команда используется для отображения общей информации о системе.

show unit

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 используется для отображения информации об устройстве.

Пример

В данном примере показано, как отобразить информацию об устройстве.

```
Switch# show unit

Model Descr                   Model Name
----------------------        ---------------
No module description         DXS-1210-16TC

Serial-Number       Status    Up Time
--------------      -------   --------------
QQDMS12345600       OK        0DT2H38M1S

Memory      Total       Used        Free
----------  ----------  ----------  ----------
DRAM        262144 k    184568 k    77576 k
FLASH       131072 k    122200 k    8872 k

Switch#
```

2.9. show cpu utilization

Данная команда используется для отображения информации 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, как получить информацию о загрузке процессора.

```
Switch#show cpu utilization

CPU Utilization

Five seconds -   8 %         One minute -   7 %         Five minutes -   7 %


Switch#
```

2.10. show version

Данная команда используется для отображения информации о версии программного обеспечения коммутатора.

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 применяется для отображения информации о версии коммутатора.

Пример

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

```
Switch# show version

System MAC Address:   00-50-43-B7-E8-02

Module Name         Versions
--------------      ----------------------
DXS-1210-16TC       H/W: B1
                    Bootloader: 1.00.001
                    Runtime: V2.00.007
Switch#
```

2.11. snmp-server enable traps environment

Данная команда позволяет получать трапы о состоянии температуры и работе вентиляторов. Для отключения данной команды воспользуйтесь формой **no**.

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

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

Параметры

fan	(Опционально) Укажите для получения трапов о состоянии вентиляторов, чтобы получать предупреждения о событиях (остановка вентилятора или восстановление работы вентилятора).
temperature	(Опционально) Укажите для получения трапов о состоянии температуры, чтобы получать предупреждение о событиях (превышение допустимых параметров температуры или восстановление температуры).

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

В данном примере показано, как включить трапы.

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

2.12. environment temperature threshold

Данная команда используется для настройки пороговых значений температуры окружающей среды. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

environment temperature threshold { low | high } <negative>

no environment temperature threshold { low | high } <negative>

Параметры

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 используется для настройки пороговых значений температуры окружающей среды внутри устройства, соответствующих 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 показано, как настроить пороговые значения температуры окружающей среды для термосенсора ID 1 в устройстве Unit 1.

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

2.13. show privilege

Данная команда используется для отображения текущего уровня привилегий.

show privilege

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 используется для отображения текущего уровня привилегий.

Пример

В данном примере показано, как отобразить текущий уровень привилегий.

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

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

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

3.2. dot1x control-direction

Данная команда используется для настройки двунаправленного (both) трафика на контролируемом порту. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

dot1x control-direction {both}

no dot1x control-direction

Параметры

both	Укажите, чтобы включить контроль трафика в двух направлениях.

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.

Пример

В данном примере показано, как настроить контроль 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 both
Switch(config-if)#
```

3.3. dot1x default

Данная команда используется для сброса 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 порте включено.

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 сброса параметров IEEE 802.1X определенного порта к настройкам по умолчанию.

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)# dot1x default
Switch(config-if)#
```

3.4. dot1x port-control

Данная команда используется для управления состоянием авторизации порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

dot1x port-control {auto | force-authorized | force-unauthorized}

no dot1x port-control

Параметры

auto	Укажите, чтобы включить аутентификацию IEEE 802.1X для порта.
force-authorized	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 показано, как запретить доступ на Ethernet-порт 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. Для отключения функции продвижения кадров dot1x PDU воспользуйтесь формой **no**.

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

mac-address *MAC-ADDRESS*	Укажите MAC-адрес для инициализации.

По умолчанию

Нет.

Режим ввода команды

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 используется для настройки максимального количества попыток для передачи клиенту запроса EAP (Extensible Authentication Protocol) от внутреннего сервера аутентификации, прежде чем инициировать повторную аутентификацию. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

dot1x max-req *TIMES*

no dot1x max-req

Параметры

TIMES	Укажите количество запросов, в которых коммутатор повторно передает кадр EAP, запрашивающему устройству перед перезапуском процесса аутентификации. Диапазон 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). Для отключения использования порта в качестве аутентификатора IEEE 802.1X воспользуйтесь формой **no**.

dot1x pae authenticator

no dot1x pae authenticator

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

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для повторной аутентификации определенного порта или 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. Для отключения аутентификации IEEE 802.1X воспользуйтесь формой **no**.

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. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

dot1x timeout {server-timeout *SECONDS* **| supp-timeout** *SECONDS* **| tx-period** *SECONDS***}**

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

Параметры

server-timeout *SECONDS*	Укажите период времени в секундах, в течение которого коммутатор ожидает запрос от сервера аутентификации. По истечении времени ожидания аутентификатор отправит клиенту пакет EAP-Request. Доступен диапазон значений от 1 до 65535.
supp-timeout *SECONDS*	Укажите период времени в секундах, в течение которого коммутатор ожидает ответ от запрашивающего устройства. По истечении времени ожидания все сообщения от запрашивающего устройства, кроме запроса EAP Request ID, будут недействительны. Доступен диапазон значений от 1 до 65535.
tx-period *SECONDS*	Укажите период времени в секундах, в течение которого коммутатор ожидает ответ на запрос EAP-Request/Identity от клиента перед повторной отправкой запроса. 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) Укажите, чтобы отобразить конфигурацию dot1x для интерфейса или группы интерфейсов. Если значение не указано, отображаться будет глобальная конфигурация.
,	(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

Любой режим конфигурирования

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 отобразить конфигурацию dot1X для интерфейса Ethernet 1/0/1.

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

Interface                  : ethernet 1/0/1
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                : Disabled

Switch#
```

3.13. show dot1x diagnostics

Данная команда используется для отображения результатов диагностики IEEE 802.1X. Если интерфейс не указан, будет отображена информация обо всех интерфейсах.

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

Параметры

interface *INTERFACE-ID*	(Опционально) Укажите, чтобы отобразить параметры диагностики dot1x на интерфейсе или группе интерфейсов. Если значение не указано, отображается информация по всем интерфейсам.
,	(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

Любой режим конфигурирования

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 будут отображаться данные диагностики для заданного интерфейса.

Пример

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

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

 ethernet 1/0/1 dot1x Diagnostics information are following:
 pnacPortAuthEntersConnecting                      : 2
 pnacPortAuthEapLogoffsWhileConnecting             : 0
 pnacPortAuthEntersAuthenticating                  : 2
 pnacPortAuthAuthSuccessWhileAuthenticating        : 0
 pnacPortAuthAuthTimeoutsWhileAuthenticating       : 0
 pnacPortAuthAuthFailWhileAuthenticating           : 0
 pnacPortAuthAuthReauthsWhileAuthenticating        : 0
 pnacPortAuthAuthEapStartsWhileAuthenticating      : 1
 pnacPortAuthAuthEapLogoffWhileAuthenticating      : 0
 pnacPortAuthAuthReauthsWhileAuthenticated         : 0
 pnacPortAuthAuthEapStartsWhileAuthenticated       : 0
 pnacPortAuthAuthEapLogoffWhileAuthenticated       : 0
 pnacPortAuthBackendResponses                      : 2
 pnacPortAuthBackendAccessChallenges               : 0
 pnacPortAuthBackendOtherRequestsToSupplicant      : 0
 pnacPortAuthBackendNonNakResponsesFromSupplicant  : 2
 pnacPortAuthBackendAuthSuccesses                  : 0
 pnacPortAuthBackendAuthFails                      : 0
Switch#
```

3.14. show dot1x statistics

Данная команда используется для отображения статистики IEEE 802.1X. Если интерфейс не указан, будет отображена информация обо всех интерфейсах.

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

Параметры

interface *INTERFACE-ID*	(Опционально) Укажите, чтобы отобразить статистику dot1x на интерфейсе или группе интерфейсов. Если значение не указано, отображается информация по всем интерфейсам.
,	(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

Любой режим конфигурирования

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. В противном случае будет отображаться статистика для заданного интерфейса.

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

ethernet 1/0/1 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. Если интерфейс не указан, будет отображена информация обо всех интерфейсах.

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

Параметры

interface *INTERFACE-ID*	(Опционально) Укажите, чтобы отобразить статистику сессии dot1x на интерфейсе или группе интерфейсов. Если значение не указано, отображается информация по всем интерфейсам.
,	(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

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения статистической информации по сессиям IEEE 802.1X. Если значение не указано, отображаться будет информация для всех интерфейсов. В противном случае будет отображаться статистика сессии для заданного интерфейса.

Пример

В данном примере показано, как вывести статистику по сессиям dot1X для Ethernet-порта 1/0/1.

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

ethernet 1/0/1 session statistic counters are following:
Octets RX                       : 0
Octets TX                       : 0
Frames RX                       : 0
Frames TX                       : 0
ID                              :
AuthenticMethod                 : Remote Authentication Server
Time                            : 0
TerminateCause                  :SupplicantLogoff
User Name                       :

Switch#
```

3.16. snmp-server enable traps dot1x

Данная команда используется для включения отправки уведомлений SNMP для аутентификации 802.1X. Для отключения отправки уведомлений SNMP воспользуйтесь формой **no**.

snmp-server enable traps dot1x

no snmp-server enable traps dot1x

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 или отключения отправки уведомлений SNMP для аутентификации 802.1X.

Пример

В данном примере показано как включить отправку трапов для аутентификации 802.1X.

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

4. Команды ACL (Список управления доступом)

4.1. access-list resequence

Данная команда используется для того, чтобы повторно задать начальный порядковый номер и для увеличения числа записей в списке доступа. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

access-list resequence {*NAME* **|** *NUMBER***}** *STARTING-SEQUENCE-NUMBER INCREMENT*

no access-list resequence

Параметры

NAME	Укажите имя конфигурируемого списка доступа. Максимальное количество символов – 32.
NUMBER	Укажите номер конфигурируемого списка доступа. Диапазон значений: от 1 до 14999.
STARTING-SEQUENCE-NUMBER	Укажите начальное значение, в соответствии с которым будут перегруппированы записи в списке. Значение по умолчанию – 10. Доступен диапазон значений от 1 до 65535.
INCREMENT	Укажите шаг для присвоения порядковых номеров. Значение по умолчанию – 10. Например, если значение шага 5, и 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 показано, как изменить порядковый номер 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 10.20.0.0 255.255.0.0
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)# rule 5 permit tcp any 10.30.0.0 255.255.0.0
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 10.30.0.0 255.255.0.0
10 permit tcp any 10.20.0.0 255.255.0.0
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 10.30.0.0 255.255.0.0
3 permit tcp any 10.20.0.0 255.255.0.0
5 permit tcp any host 10.100.1.2
7 permit icmp any any
Switch(config)#
```

4.2. acl-hardware-counter

Данная команда используется для включения аппаратного счетчика ACL (ACL hardware counter) указанного списка доступа для функций группы доступа (access group). Для отключения аппаратного счетчика ACL воспользуйтесь формой **no**.

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

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

Параметры

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

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

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

В данном примере показано, как включить аппаратный счетчик ACL.

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

4.3. clear acl-hardware-counter

Данная команда используется для обнуления аппаратных счетчиков ACL.

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

Параметры

access-group *ACCESS-LIST-NAME*	Укажите имя удаляемого списка доступа.
access-group *ACCESS-LIST-NUMBER*	Укажите номер настраиваемого списка доступ.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если в параметре **access-group** не указано определенное имя (access-list name) или номер списка доступа (access-list number), данная команда обнулит аппаратные счетчики сразу для всех списков управления доступом (access-group hardware counters).

Пример

В данном примере показано, как обнулить аппаратные счетчики ACL.

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

4.4. expert access-group

Данная команда используется для применения указанных списков управления доступом expert (expert ACL) к интерфейсу. Для отмены применения воспользуйтесь формой **no**.

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

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

Параметры

NAME	Укажите имя настраиваемого списка управления доступом expert (expert access-list). Максимальное число допустимых символов в имени – 32.
NUMBER	Укажите номер настраиваемого списка управления доступом expert (expert access-list).
in	(Опционально) Фильтрация входящих пакетов на интерфейсе. 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 expert (expert access group) уже настроена на интерфейсе, команда, применяемая позже, перезапишет 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.

Пример

В данном примере показано, как применить список управления доступом expert к интерфейсу. Применяется ACL **exp_acl** на порту 1/0/2 для фильтрации входящих пакетов.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# expert access-group exp_acl in
Switch(config-if)# end
Switch# show access-group interface ethernet 1/0/2
ethernet 1/0/2:
  Inbound expert access-list : exp_acl(ID: 8999)
Switch#
```

4.5. 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. Для удаления расширенного списка управления доступом expert воспользуйтесь формой **no**.

expert access-list extended *NAME* **[***NUMBER***]**

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

Параметры

NAME	Укажите имя конфигурируемого расширенного списка управления доступом expert. Максимальное число допустимых символов в имени – 32.
NUMBER	Укажите 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#
```

4.6. ip access-group

Данная команда используется для указания списка доступа IP (IP access list), который будет применяться к интерфейсу. Для удаления списка доступа IP воспользуйтесь формой **no**.

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

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

Параметры

NAME	Укажите имя используемого списка доступа IP. Максимальное число допустимых символов в имени – 32.
NUMBER	Укажите номер используемого списка доступа IP.
in	(Опционально) Указывает, что список доступа IP 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 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 показано, как настроить список 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 526
Switch(config-if)#
```

4.7. 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. Для удаления списка доступа IP воспользуйтесь формой **no**.

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	Укажите имя конфигурируемого списка доступа IP. Максимальное число допустимых символов в имени – 32. Первым символом должна быть буква.
NUMBER	Укажите ID-номер (ID number) списка доступа IP. Для стандартных списков доступа IP диапазон значений от 1 до 1999. Для расширенных списков доступа IP диапазон значений от 2000 до 3999.

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 IP.

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
Swtich(config-ip-ext-acl)# rule permit tcp any 10.20.0.0 255.255.0.0
Swtich(config-ip-ext-acl)# exit
Swtich(config)# ip access-list pim-srcfilter
Switch(config-ip-acl)# rule permit host 172.16.65.193 any
Switch(config-ip-acl)#
```

4.8. ipv6 access-group

Данная команда используется для применения списка доступа IPv6 (IPv6 access list) на интерфейсе. Для удаления списка доступа IPv6 воспользуйтесь формой **no**.

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

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

Параметры

NAME	Укажите имя используемого списка доступа IPv6.
NUMBER	Укажите номер используемого списка доступа IPv6.
in	(Опционально) Указывает, что список доступа IPv6 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

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

```
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 156
Switch(config-if)#
```

4.9. 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. Для удаления списка доступа IPv6 воспользуйтесь формой **no**.

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	Укажите имя конфигурируемого списка доступа IPv6. Максимальное число допустимых символов в имени –

	32.
NUMBER	Укажите ID-номер (ID number) списка доступа IPv6. Для стандартных списков доступа IPv6 диапазон значений от 11000 до 12999. Для расширенных списков доступа IPv6 диапазон значений от 13000 до 14999.

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 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
Swtich(config-ipv6-ext-acl)# rule 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
Swtich(config-ipv6-acl)# rule permit any fe80::101:1/54
Switch(config-ipv6-acl)#
```

4.10. list-remark

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

list-remark *TEXT*

no list-remark

Параметры

TEXT	Укажите текст комментария. Текст может содержать не более 256 символов.

По умолчанию

Нет.

Режим ввода команды

Access-list Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

```
Switch# configure terminal
Switch(config)#ip access-list extended R&D
Switch(config-ip-ext-acl)# list-remark "This access-list is used to match ar
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#
```

4.11. 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, как применить список доступа MAC daily-profile к Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)# mac access-group daily-profile in
The remaining applicable MAC access entries are 204
Switch(config-if)#
```

4.12. 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)#
```

4.13. 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-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.
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.
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.
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, router-solicitation, time-exceeded, 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
```

4.14. 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***} [fragments] [[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*] **[fragments] [[precedence** *PRECEDENCE*] **[tos** *TOS*] **| dscp** *DSCP*] **[time-range** *PROFILE-NAME*]

Стандартный список доступа IP (Standard IP Access List):

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***] [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	Указывает на любой IP-адрес источника или IP-адрес назначения.
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.
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.
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.
tcp, udp, igmp, ipinip, gre, esp, eigrp, ospf, pcp, pim, vrrp	Укажите протоколы 4 уровня.
PROTOCOL-ID	Укажите Protocol ID. Доступен диапазон значений от 0 до 255.
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: 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)#
```

4.15. 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):

rule [*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***] [***TCP-FLAG***] [dscp** *VALUE***] [flow-label** *FLOW-LABEL***] [time-range** *PROFILE-NAME***]**

rule [*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***] [flow-label** *FLOW-LABEL***] [time-range** *PROFILE-NAME***]**

rule [*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***] [flow-label** *FLOW-LABEL***] [time-range** *PROFILE-NAME***]**

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

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

Стандартный список доступа IPv6 (Standard IPv6 Access List):

rule [*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	Указывает на любой IPv6-адрес источника или IPv6-адрес назначения.
host *SRC-IPV6-ADDR*	Укажите конкретный IPv6-адрес узла источника.
SRC-IPV6-ADDR/PREFIX-LENGTH	Укажите сеть IPv6 источника.
host *DST-IPV6-ADDR*	Укажите конкретный 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.
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.
time-range *PROFILE-NAME*	(Опционально) Укажите имя профиля периода времени, связанного со списком доступа, определяющим период его активации.

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)#
```

4.16. 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***] [vlan** *VLAN-ID***] [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	Указывает на любой MAC-адрес источника или MAC-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-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)#
```

4.17. 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
Любой режим конфигурирования

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

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

Switch#
```

4.18. 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): ethernet 1/0/5-ethernet 1/0/8

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. ip http server

Данная команда используется для включения сервера HTTP. Для отключения сервера HTTP воспользуйтесь формой **no**.

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 показано, как включить сервер HTTP.

```
Switch# configure terminal
Switch(config)#ip http server
The SSL function will be set to disable.
Switch(config)#
```

5.3. ip http secure-server

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

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

no ip http secure-server

Параметры

POLICY-NAME	(Опционально) Укажите имя политики SSL Service Policy. Используйте параметр **ssl-service-policy**, только если вы уже указали политику SSL Service Policy с помощью команды **ssl-service-policy**. Если данный параметр не

	указан, будет использоваться встроенный локальный сертификат для HTTPS.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда позволяет включить сервер HTTPS и использовать указанную политику SSL Service Policy для HTTPS.

Пример

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

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

5.4. ip http access-class

Данная команда используется для указания списка, которому необходимо ограничить доступ к HTTP-серверу. Для отмены проверки при помощи списка доступа воспользуйтесь формой **no**.

ip http access-class *IP-ACL*

no ip http access-class *IP-ACL*

Параметры

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

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

В данном примере показан процесс создания стандартного списка доступа и назначение его для доступа к HTTP-серверу. Только узлу 226.1.1.1 разрешен доступ к серверу.

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

5.5. ip http service-port

Данная команда используется для указания порта HTTP. Для возврата к настройкам по умолчанию (порт 80) воспользуйтесь формой **no**.

ip http service-port *TCP-PORT*

no ip http service-port

Параметры

TCP-PORT	Укажите 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 показано, как настроить TCP-порт 8080 для HTTP.

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

5.6. ip http timeout-policy idle

Данная команда используется для установки значения тайм-аута простоя (idle timeout) для подключения к серверу HTTP в секундах. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

ip http timeout-policy idle *INT*

no ip http timeout-policy idle

Параметры

INT	Укажите значение тайм-аута простоя. 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 используется для настройки значения тайм-аута простоя для подключения к серверу HTTP.

Пример

В данном примере показано, как настроить тайм-аут простоя со значением 100 секунд.

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

5.7. ip telnet server

Данная команда используется для включения сервера Telnet. Для отключения сервера Telnet воспользуйтесь формой **no**.

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 показано, как включить сервер Telnet.

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

5.8. ip telnet service-port

Данная команда используется для указания сервисного порта для Telnet. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

ip telnet service-port *TCP-PORT*

no ip telnet service-port

Параметры

TCP-PORT	Укажите 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 показано, как настроить сервисный порт 3000 для Telnet.

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

5.9. line

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

line {console | telnet ssh}

Параметры

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

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда позволяет войти в режим Line Configuration Mode.

Пример

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

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

5.10. service password-encryption

Данная команда используется для включения шифрования пароля перед сохранением в файле конфигурации. Для отключения шифрования воспользуйтесь формой **no**.

service password-encryption {7 | 15}

no service password-encryption

Параметры

7	Укажите пароль, зашифрованный на основе SHA-1.
15	Укажите пароль, зашифрованный на основе MD5.

По умолчанию

Нет.

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 последней опцией шифрования пароля, 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 показано, как включить шифрование SHA-1 пароля перед сохранением в файле конфигурации.

```
Switch# configure terminal
Switch(config)# service password encryption 7
Switch(config)#
```

5.11. 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

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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

```
Switch# show terminal

Terminal Settings:
Length: 25 lines
Width: 80 columns
Default Length: 25 lines
Default Width: 80 columns
Baud rate: 115200 bps

Switch#
```

5.12. show ip telnet server

Данная команда используется для получения информации о состоянии сервера Telnet.

show ip telnet server

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 применяется для отображения информации о состоянии сервера Telnet.

Пример

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

```
Switch# show ip telnet server

Server State: Enabled

Switch#
```

5.13. show ip http server

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

show ip http server

Параметры

Нет.

По умолчанию

По умолчанию отображение информации о состоянии включено.

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 состоянии HTTP-сервера.

Пример

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

```
Switch#show ip http server

ip http server state :  enable
Switch#
```

5.14. 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

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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

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

Total Entries: 1

Switch#
```

5.15. terminal length

Данная команда используется для настройки количества строк, отображаемых на экране. Команда **terminal length** влияет только на текущую сессию. Команда **terminal length default** установит значение по умолчанию, но не повлияет на текущую сессию. Созданный

заново терминал будет использовать значение по умолчанию. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

terminal length *NUMBER*

no terminal length

Параметры

NUMBER	Укажите количество строк, отображаемых 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

EXEC Mode или Privilege EXEC Mode для команды **terminal length**.

Уровень команды по умолчанию

Уровень 1 для команды **terminal length**.

Использование команды

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

Если для terminal length указано значение, отличное от 0, например 50, то отображение будет останавливаться после каждых 50 строк. Данная команда используется для настройки количества строк, 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 вернуться к 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.

Пример

В данном примере показано, как изменить количество строк на 60.

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

5.16. session timeout

Данная команда позволяет задать значение тайм-аута сессии (консольной сессии, сессии терминала Telnet, сессии терминала SSH). Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

session-timeout *MINUTES*

no session-timeout

Параметры

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

По умолчанию

Значение по умолчанию – 3 минуты.

Режим ввода команды

Line Configuration Mode.

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 показано, как настроить 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)#
```

5.17. terminal width

Данная команда используется для настройки количества столбцов символов, отображаемых на экране для текущей сессии. Команда **terminal width** влияет только на текущую сессию.

terminal width *NUMBER*

no terminal width

Параметры

NUMBER	Укажите количество символов, отображаемых на экране. Допустимы значения от 40 до 255.

По умолчанию

Значение по умолчанию – 80.

Режим ввода команды

EXEC Mode или Privilege EXEC Mode для команды **terminal width**.

Уровень команды по умолчанию

Уровень 1 (для команды **terminal width**).

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.

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 показано, как изменить текущую ширину терминала на 120.

```
Switch# show terminal

Terminal Settings:
Length: 25 lines
Width: 80 columns
Default Length: 25 lines
Default Width: 80 columns
Baud rate: 115200 bps

Switch# terminal width 120
Switch# show terminal

Terminal Settings:
Length: 25 lines
Width: 120 columns
Default Length: 25 lines
Default Width: 80 columns
Baud rate: 115200 bps

Switch #
```

5.18. username

Данная команда используется для создания учетной записи пользователя. Для удаления учетной записи пользователя воспользуйтесь формой **no**.

username *NAME* **[privilege** *LEVEL***] [nopassword | password [0 | 7 | 15]** *PASSWORD***]**

no username [*NAME***]**

Параметры

NAME	Укажите имя пользователя, максимум 32 символа.
privilege *LEVEL*	(Опционально) Укажите уровень привилегий 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) Укажите 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) Укажите 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) Укажите 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) Укажите пароль на основе одного из указанных выше параметров.

По умолчанию

По умолчанию имя пользователя – *admin*, пароль – *admin*, уровень привилегий – 15.

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

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

В данном примере показано, как удалить учетную запись администратора с именем **admin.**

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

5.19. show user-account

Данная команда используется для отображения информации об учетных записях пользователей, созданных на коммутаторе.

show user-account

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 используется для отображения информации об учетных записях пользователей, созданных на коммутаторе.

Пример

В данном примере показано, как отобразить всю информацию об учетных записях пользователей.

```
Switch# show user-account
User Name           Privilege  Password  Password Type
------------------  ---------  --------  -------------
admin               15         ******    Plain Text

Total Entries: 1

Switch#
```

5.20. show service password-encryption

Данная команда используется для отображения информации о состоянии функции «шифрование пароля».

show service password-encryption

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 используется для отображения информации о состоянии функции «шифрование пароля».

Пример

В данном примере показано, как отобразить информацию о состоянии функции «шифрование пароля».

```
Switch# show service password-encryption

Password Encryption State: Disabled
Switch#
```

5.21. show session-timeout

Данная команда используется для отображения информации о тайм-ауте сессии.

show session-timeout

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 используется для отображения информации о тайм-ауте сессии.

Пример

В данном примере показано, как отобразить информацию о тайм-ауте сессии.

```
Switch# show session-timeout

Web Session Timeout     (second): 180
Telnet Session Timeout  (minute): 30
Console Session Timeout (minute): 30
SSH Session Timeout     (minute): 30

Switch#
```

5.22. show ip {http | telnet} service-port

Данная команда используется для отображения информации о сервисном порту HTTP или Telnet.

show ip {http | telnet} service-port

Параметры

http	Укажите для отображения информации о сервисном порту HTTP.
telnet	Укажите для отображения информации о сервисном порту Telnet.

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 сервисном порту HTTP или Telnet.

Пример

В данном примере показано, как отобразить сервисный порт HTTP.

```
Switch# show ip http service-port

IP HTTP server port : 80
Switch#
```

5.23. ping access-class

Данная команда используется для указания списка, с помощью которого можно ограничить ping до коммутатора. Для отмены проверки списка доступа воспользуйтесь формой **no**.

ping access-class *IP-ACL*

no ping 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

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для указания списка доступа, с помощью которого можно ограничить ping до коммутатора. Для отмены проверки списка доступа воспользуйтесь формой **no**.

Пример

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

```
Switch# configure terminal
Switch(config)#ip access-list ping-filter
Switch(config-ip-acl)#rule permit 226.1.1.1 255.255.255.0
Switch(config-ip-acl)# exit
Switch(config)# ping access-class ping-filter
Switch(config)#
```

5.24. ip https access-class

Данная команда используется для указания списка, с помощью которого можно ограничить доступ к HTTPS-серверу. Для отмены проверки при помощи списка доступа воспользуйтесь формой **no**.

ip https access-class *IP-ACL*

no ip https 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

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для указания списка, с помощью которого можно ограничить доступ к HTTPS-серверу. Для отмены проверки при помощи списка доступа воспользуйтесь формой **no**.

Пример

В данном примере показан процесс создания стандартного списка доступа и назначение его для ограничения доступа к HTTPS-серверу. Только узлу 226.1.1.1 разрешен доступ к серверу.

```
Switch# configure terminal
Switch(config)#ip access-list https-filter
Switch(config-ip-acl)#rule permit 226.1.1.1 255.255.255.0
Switch(config-ip-acl)# exit
Switch(config)# ip https access-class https-filter
Switch(config)#
```

5.25. show trusted host

Данная команда используется для отображения информации о доверенном узле Telnet, Ping, HTTP, HTTPS.

show trusted host [telnet | ping | http | https]

Параметры

telnet	Укажите информацию о доверенном узле Telnet.
ping	Укажите информацию о доверенном узле Ping.
http	Укажите информацию о доверенном узле HTTP Telnet.
https	Укажите информацию о доверенном узле HTTPS Telnet.

По умолчанию

Показана вся информация о доверенном узле.

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 доверенном узле для Telnet, Ping, HTTP, HTTPS.

Пример

В данном примере показано, как отобразить информацию о доверенном узле HTTPS.

```
Switch# show trusted host https
Type    ACL Name
------  --------------------------------
https   https-filter

Total Entries: 1

Switch#
```

6. Команды Asymmetric VLAN

6.1. asymmetric-vlan

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

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 данную команду для включения/отключения функции Asymmetric VLAN.

Пример

В данном примере показано, как включить функцию Asymmetric VLAN.

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

В данном примере показано, как отключить функцию Asymmetric VLAN.

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

6.2. show asymmetric-vlan

Данная команда используется для отображения информации об Asymmetric VLAN.

show asymmetric-vlan

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 используется для отображения информации об Asymmetric VLAN.

Пример

В данном примере показано, как отобразить информацию об Asymmetric VLAN.

```
Switch# show asymmetric-vlan

Asymmetric VLAN State: Disabled

Switch#
```

7. Команды Authentication, Authorization, and Accounting (AAA)

7.1. aaa authentication dot1x

Данная команда используется для настройки списка методов по умолчанию, используемого для аутентификации 802.1X. Для удаления списка методов по умолчанию воспользуйтесь формой **no**.

aaa authentication dot1x default *METHOD1* **[***METHOD2...]*

no aaa authentication dot1x defaulta

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)#
```

7.2. 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. Для удаления группы серверов RADIUS воспользуйтесь формой **no**.

aaa group server radius *GROUP-NAME*

no aaa group server radius *GROUP-NAME*

Параметры

GROUP-NAME	Укажите 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

Данная команда используется 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 данная команда используется 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)#
```

7.3. aaa new-model

Данная команда используется для включения AAA для аутентификации и аккаунтинга. Для отключения функции AAA воспользуйтесь формой **no**.

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

Данная команда используется 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)#
```

7.4. radius-server deadtime

Данная команда используется для указания времени по умолчанию, по истечении которого сервер, который не может ответить, будет пропущен. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

radius-server deadtime *MINUTES*

no radius-server deadtime

Параметры

MINUTES	Укажите время простоя. Допустимый 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)#
```

7.5. radius-server host

Данная команда используется для создания узла сервера RADIUS. Для удаления узла сервера воспользуйтесь формой **no**.

radius-server host {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [auth-port** *PORT***]**

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

Параметры

IP-ADDRESS	Укажите IP-адрес сервера RADIUS.
IPV6-ADDRESS	Укажите IPv6-адрес сервера RADIUS.
auth-port *PORT-NUMBER*	(Опционально) Укажите номер UDP-порта назначения для отправки пакетов аутентификации. Диапазон: от 0 до 65535. Установите номер порта в ноль, если узел сервера не предназначен для аутентификации. Значение по умолчанию: 1812.

По умолчанию

По умолчанию сервер не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда используется 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)#
```

7.6. server (RADIUS)

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

server {*IP-ADDRESS* **|** *IPV6-ADDRESS***}**

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

Параметры

IP-ADDRESS	Укажите IPv4-адрес сервера аутентификации.

IPV6-ADDRESS	Укажите IPv6-адрес сервера аутентификации.

По умолчанию

По умолчанию сервер не настроен.

Режим ввода команды

RADIUS Group Server Configuration Mode

Уровень команды по умолчанию

Уровень 15.

Использование команды

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. 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 re
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)# exit
Switch(config)#
```

7.7. server (TACACS+)

Данная команда используется для связывания сервера TACACS+ с группой серверов. Для удаления сервера из группы серверов воспользуйтесь формой **no**.

server {*IP-ADDRESS* **|** *IPV6-ADDRESS***}**

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

Параметры

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

По умолчанию

По умолчанию сервер не настроен.

Режим ввода команды

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 узла сервера. 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+)# exit
Switch(config)#
```

7.8. show aaa

Данная команда используется для отображения глобального состояния AAA.

show aaa

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privilege EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения глобального состояния AAA.

Пример

В данном примере показано, как отобразить глобальное состояние AAA.

```
Switch# show aaa

AAA is enabled.

Switch#
```

7.9. 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

Privilege EXEC Mode

Любой режим конфигурирования

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
                               Auth.
Round Trip Time:               10
Access Requests:                4
Access Accepts:                 0
Access Rejects:                 4
Access Challenges:              0
Acct Request:                  NA
Acct Response:                 NA
Retransmissions:                0
Malformed Responses:            0
Bad Authenticators:             0
 Pending Requests:              0
 Timeouts:                      0
 Unknown Types:                 0
 Packets Dropped:               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, или 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, полученных от данного сервера и отброшенных по какой-либо причине.

7.10. aaa authentication login

Данная команда используется для указания определенного метода аутентификации при входе в систему. Для удаления методов воспользуйтесь формой **no**.

aaa authentication login {default | *LIST-NAME***}** *METHOD1* **[***METHOD2...***]**

no aaa authentication login {default | *LIST-NAME***}**

Параметры

default	Укажите, чтобы использовать для аутентификации список методов по умолчанию.

METHOD-LIST	Укажите, чтобы использовать для аутентификации определенный метод.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда используется для указания метода аутентификации при входе в систему (SSH, консоль и Telnet).

Пример

В данном примере показано, как настроить метод с именем «test» для входа по SSH.

```
Switch(config)# aaa authentication login test radius
Switch(config)# line ssh
Switch(config-line)# login authentication test
```

7.11. http login authentication method

Данная команда используется для применения определенного метода для входа в HTTP-сессию.

ip http authentication aaa login-authentication {default | *METHOD-LIST***}**

no ip http authentication aaa login-authentication

Параметры

default	Укажите, чтобы использовать для аутентификации список методов по умолчанию.
METHOD-LIST	Укажите, чтобы использовать для аутентификации определенный метод.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда используется для применения определенного метода для входа в HTTP-сессию.

Пример

В данном примере показано, как настроить метод с именем «test» для входа по HTTP.

```
Switch(config)# aaa authentication login test tacacs+
Switch(config)# ip http authentication aaa login-authentication test
Switch(config)# show aaa
```

8. Базовые команды настройки IPv4

8.1. arp

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

arp *IP-ADDRESS HARDWARE-ADDRESS*

no arp *IP-ADDRESS HARDWARE-ADDRESS*

Параметры

IP-ADDRESS	Укажите IP-адрес сетевого уровня.
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 данном примере показано, как добавить статическую ARP-запись для традиционного Ethernet-узла.

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

8.2. arp timeout

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

arp timeout *MINUTES*

no arp timeout

Параметры

MINUTES	Укажите таймаут, по истечении которого динамическая запись устареет при условии отсутствия сетевой активности. Допустимые значения – от 0 до 65535.

По умолчанию

По умолчанию установлено 20 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. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

Пример

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

```
Switch# configure terminal
Switch(config)#interface vlan1
Switch(config-if)# arp timeout 60
Switch(config-if)#
```

8.3. 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#
```

8.4. ip address

Данная команда используется для назначения интерфейсу первичного или вторичного адреса IPv4 или автоматического получения IP-адреса от DHCP-сервера. Для удаления настройки IP-адреса или отключения DHCP на интерфейсе воспользуйтесь формой **no**.

ip address {*IP-ADDRESS SUBNET-MASK* **| dhcp}**

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

Параметры

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

По умолчанию

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

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

IPv4-адрес интерфейса может быть задан пользователем вручную или динамически (автоматически) назначен сервером DHCP. При настройке вручную пользователь может назначить в одну VLAN сразу несколько сетей с IP-адресом для каждой. Один из этих IP-адресов должен быть основным IP-адресом, а остальные – второстепенными. Основной адрес используется в качестве IP-адреса источника для отправленных с интерфейса сообщений SNMP Trap или SYSLOG. Используйте команду **no ip address** для удаления заданного IP-адреса.

Пример

В данном примере показано, как настроить 10.108.1.27 в качестве основного адреса.

```
Switch# configure terminal
Switch(config)#interface vlan100
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
Switch(config-if)# ip address 192.31.8.17 255.255.255.0
Switch(config-if)#
```

8.5. show arp

Данная команда используется для отображения данных кэша ARP.

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

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#
```

8.6. show arp timeout

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

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

Параметры

INTERFACE-ID	Укажите идентификатор интерфейса (ID).

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 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#
```

8.7. 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 краткую информацию по IP-интерфейсу.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

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 всех интерфейсов.

```
Switch#show ip interface

Interface vlan1 is enabled, Link status is up
  IP Address is 10.90.90.90/8 (Manual)
  ARP timeout is 20 minutes.

Total Entries: 1

Switch#
```

8.8. ip enable

Данная команда используется для включения IP-интерфейса. Для отключения IP-интерфейса воспользуйтесь формой **no**.

ip enable

no ip enable

Параметры

Нет.

По умолчанию

По умолчанию включено.

Режим ввода команды

VLAN Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

IPv4-адрес интерфейса может быть задан пользователем вручную или динамически (автоматически) назначен сервером DHCP. При настройке вручную пользователь может назначить в одну VLAN сразу несколько сетей с IP-адресом для каждой. Один из этих IP-адресов должен быть основным IP-адресом, а остальные – второстепенными. Основной

адрес используется в качестве IP-адреса источника для отправленных с интерфейса сообщений SNMP Trap или SYSLOG. Используйте команду **no ip address** для отключения IP-интерфейса.

Пример

В данном примере показано, как включить IP-интерфейс.

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

9. Базовые команды настройки IPv6

9.1. clear ipv6 neighbors

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

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

Параметры

all	Укажите, чтобы удалить динамические записи из IPv6 neighbor cache для всех интерфейсов.
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 данном примере показано, как очистить IPv6 neighbor cache для интерфейса VLAN 1.

```
Switch# enable
Switch# clear ipv6 neighbors vlan1
Switch#
```

9.2. ipv6 address

Данная команда используется для ручной настройки IPv6-адреса на интерфейсе. Для удаления заданного вручную IPv6-адреса воспользуйтесь формой **no**.

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). Однако в пределах одного и того же префикса можно настроить только один IPv6-адрес.

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

Пример

В данном примере показано, как настроить IPv6-адрес.

```
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
```

9.3. 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

Нет.

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)#
```

9.4. ipv6 enable

Данная команда используется для включения обработки IPv6 на интерфейсах, у которых нет явно настроенного IPv6-адреса. Для отключения обработки IPv6 на интерфейсах, у которых нет явно настроенного IPv6-адреса воспользуйтесь формой **no**.

ipv6 enable

no ipv6 enable

Параметры

Нет.

По умолчанию

По умолчанию данная опция выключена.

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)#
```

9.5. ipv6 neighbor

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

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

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

Команда **clear ipv6 neighbors** позволит удалить динамические записи из таблицы IPv6 neighbor. Для удаления статической записи используйте команду **no ipv6 neighbor**.

Пример

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

```
Switch# configure terminal
Switch(config)#ipv6 neighbor fe80::1 vlan1 00-01-80-11-22-99
Switch(config)#
```

9.6. 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

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для просмотра настроек конфигурации IPv6-интерфейса.

Пример

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

```
Switch# show ipv6 interface vlan 2

vlan2 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)
  RA advertised retransmit interval is 0 milliseconds

Switch#
```

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

```
Switch# show ipv6 interface brief

vlan1 is up, Link status is up
    FE80::201:1FF:FE02:304

vlan2 is up, Link status is down
    FE80::201:1FF:FE02:305
    200::2

vlan3 is up, Link status is down
    FE80::201:1FF:FE02:306

Total Entries: 3

Switch#
```

9.7. show ipv6 neighbors

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

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

Параметры

IPV6-ADDRESS	Укажите IPv6-адрес, чтобы получить для него

	информацию о записях в таблице IPv6 neighbor cache.
INTERFACE-ID	Укажите интерфейс для отображения информации о записях в таблице IPv6 neighbor cache.

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 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 Sta
--------------------------------------- ----------------- --------- ---- ---
FE80::200:11FF:FE22:3344                00-00-11-22-33-44 vlan1     D   REAC

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 момента получения последнего подтверждения прошло

	больше заданного таймером Reachable Time времени (в миллисекундах). **PROBE** – состояние записи, при котором устройство отправляет сообщение Neighbor Solicitation, чтобы подтвердить достижимость.

9.8. ipv6 nd ns-interval

Данная команда используется для установки интервала повторной передачи сообщений NS (Neighbor Solicitation).

ipv6 nd ns-interval *INTERVAL*

no ipv6 nd ns-interval

Параметры

INTERVAL	Интервал повторной передачи в миллисекундах.

По умолчанию

Нет.

Режим ввода команды

VLAN Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для установки интервала повторной передачи сообщений NS (Neighbor Solicitation).

Пример

В данном примере показано, как установить интервал повторной передачи сообщений NS.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 nd ns-interval 1200
Switch(config-if)#
```

10. Команды Cable Diagnostics

10.1. 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 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 в одной 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 состояния и длины медных кабелей.

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

10.2. 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 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

В данном примере показано, как отобразить результаты тестирования диагностики кабеля.

```
Switch# show cable-diagnostics

Port      Type       Link Status    Test Result                    Cable Length (M)
------  ----------  -------------  -----------------------------  ----------------
-
ethernet 1/0/1     1000BASE-T  Link Up        OK                                65
ethernet 1/0/2     1000BASE-T  Link Up        OK                                 -
ethernet 1/0/3     1000BASE-T  Link Down      Shutdown                          25
ethernet 1/0/4     1000BASE-T  Link Down      Shutdown                           -
ethernet 1/0/5     1000BASE-T  Link Down      Unknown                            -
ethernet 1/0/6     1000BASE-T  Link Down      Pair 1 Crosstalk at  30M           -
                                              Pair 2 Crosstalk at  30M
                                              Pair 3 OK         at 110M
                                              Pair 4 OK         at 110M
ethernet 1/0/7     1000BASE-T  Link Down      NO Cable                           -
ethernet 1/0/8     1000BASE-T  Link Down      Pair 1 Open       at  16M          -
                                              Pair 2 Open       at  16M
                                              Pair 3 OK         at  50M
                                              Pair 4 OK         at  50M

Switch#
```

10.3. clear cable-diagnostics

Данная команда используется для очистки результатов диагностики кабеля.

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

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#
```

11. Команды Dynamic ARP Inspection

11.1. arp access-list

Данная команда используется для создания или изменения списка доступа ARP. Команда позволяет войти в режим ARP Access-list Configuration Mode. Для удаления списка доступа ARP воспользуйтесь формой **no**.

arp access-list *NAME*

no arp access-list *NAME*

Параметры

NAME	Укажите имя списка доступа ARP, 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

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 test
Switch(config-arp-nacl)# permit ip 192.168.0.113 255.255.255.0 mac any
```

11.2. clear 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#
```

11.3. clear 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*	(Опционально) Укажите VLAN или диапазон VLAN.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

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#
```

11.4. ip arp inspection filter vlan

Данная команда позволяет указать список доступа ARP, который будет использоваться для проверки ARP Inspection для VLAN. Для удаления указанной привязки воспользуйтесь формой **no**.

ip arp inspection filter *ARP-ACL-NAME* **vlan** *VLAN-ID* **[, | -] [static]**

no ip arp inspection filter *ARP-ACL-NAME* **vlan** *VLAN-ID* **[, | -] [static]**

Параметры

ARP-ACL-NAME	Укажите имя списка управления доступом. Максимально допустимое количество символов – 32.
vlan *VLAN-ID*	Укажите VLAN, сопоставленную со списком доступа ARP.
,	(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.
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 на 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 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)#
```

11.5. ip arp inspection limit

Данная команда используется для ограничения скорости входящих ARP-запросов и ответов на интерфейсе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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. Доступный диапазон значений: от 1 до 150.
burst interval *SECONDS*	(Опционально) Укажите разрешенную величину продолжительности всплеска (burst duration) ARP-пакетов. Диапазон значений: от 1 до 15. Если не указано, значение по умолчанию составляет 1 секунду.
none	Укажите, чтобы скорость передачи ARP-пакетов не была ограничена.

По умолчанию

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 последующих 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)#
```

11.6. ip arp inspection trust

Данная команда используется для назначения доверенного интерфейса для Dynamic ARP Inspection. Для отключения режима доверенного интерфейса воспользуйтесь формой **no**.

ip arp inspection trust

no ip arp inspection trust

Параметры

Нет.

По умолчанию

По умолчанию данная функция 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 1/0/10 для DAI.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/10
Switch(config-if)# ip arp inspection trust
Switch(config-if)#
```

11.7. ip arp inspection validate

Данная команда используется для указания дополнительных проверок при ARP Inspection. Для отключения дополнительных проверок воспользуйтесь формой **no**.

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, и IP-адрес назначения в ARP-ответе. Пакеты, отправляемые на IP-адреса 0.0.0.0, 255.255.255.255 и все IP-адреса многоадресной рассылки отбрасываются. IP-адреса источника проверяются во всех ARP-запросах и ответах, а IP-адреса назначения проверяются только в ARP-ответах.

По умолчанию

По умолчанию данная функция 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 параметры не указаны, все опции включены или выключены. Для отключения определенных типов проверок воспользуйтесь формой **no**.

Пример

В данном примере показано, как включить проверку MAC-адреса источника.

```
Switch# configure terminal
Switch(config)# ip arp inspection validate src-mac
Switch(config)#
```

11.8. ip arp inspection vlan

Данная команда используется для включения Dynamic ARP Inspection для определенных VLAN. Для отключения Dynamic ARP Inspection для VLAN воспользуйтесь формой **no**.

ip arp inspection vlan vlan *VLAN-ID* **[, | -]**

no ip arp inspection vlan vlan *VLAN-ID* **[, | -]**

Параметры

vlan *VLAN-ID*	Укажите VLAN или диапазон VLAN.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию функция 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)#
```

11.9. ip arp inspection vlan logging

Данная команда используется для управления типом пакетов, которые будут регистрироваться (логироваться). Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

ip arp inspection vlan *VLAN-ID* **[, | -] logging {acl-match {deny | permit | all | none} | dhcp-bindings {deny | permit | all | none}}**

no ip arp inspection vlan *VLAN-ID* **[, | -] logging {acl-match | dhcp-bindings}**

Параметры

vlan *VLAN-ID*	Укажите VLAN или диапазон VLAN.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
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** для возврата команды к критериям логирования по умолчанию.

Пример

В данном примере показано, как настроить ARP Inspection в VLAN 1 для добавления пакетов в журнал на основе списка управления доступом (ACL).

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 1 logging acl-match all
Switch(config)#
```

11.10. permit | deny (arp access-list)

Данная команда применяется для управления доступом ARP-записи. Используйте команду **deny** для создания запрещающей ARP-записи. Для удаления записи воспользуйтесь формой **no**.

{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 разрешенными записями.

```
Switch# configure terminal
Switch(config)# arp access-list test
Switch(config-arp-nacl)# permit ip 192.168.0.113 255.255.255.0 mac any
```

11.11. show ip arp inspection

Данная команда используется, чтобы отобразить статус DAI для указанного диапазона VLAN.

show ip arp inspection [interfaces [*INTERFACE-ID* **[, | -]] | statistics [vlan** *VLAN-ID* **[, | -]]]}**

Параметры

interfaces *INTERFACE-ID*	(Опционально) Укажите интерфейс (порт) или диапазон интерфейсов (портов).
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
statistics	(Опционально) Данные статистики DAI.
vlan *VLAN-ID*	(Опционально) Укажите VLAN или диапазон VLAN.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется, чтобы отобразить статус DAI для указанного диапазона VLAN.

Пример

В данном примере показано, как отобразить конфигурацию и рабочее состояние 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#
```

12. Команды Debug

12.1. debug show tech-support

Данная команда используется для отображения информации, запрашиваемой техническим персоналом.

debug show tech-support

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 15.

Использование команды

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

Пример

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

```
Switch# debug show tech-support
#------------------------------------------------------------------
# DXS-1210-16TC 10GbE Smart Managed Switch
# Technical Support Information
#
# Firmware:  V2.00.007
# Copyright(C) 2021 D-Link Corporation. All rights reserved.
#------------------------------------------------------------------
******************** Basic System Information ********************
Boot Time                              :0 days, 1 hrs, 36 min, 20 secs
RTC Time                               :01/01/2021 01:36:13
Boot PROM Version                      :V1.00.001
Firmware Version                       :V2.00.007
Hardware Version                       :B1
MAC Address                            :00-50-43-B7-E8-02
Serial Number                          :QQDMS12345600
SNMP Status                            :Disabled
Safeguard Engine                       :Enabled
IGMP Snooping                          :Disabled
Scheduled Port-shutdown Power Saving :Disabled
Scheduled Hibernation Power Saving   :Disabled
Scheduled Dim-LED Power Saving       :Disabled
Administrative Dim-LED                 :Disabled

#------------------------------------------------------------------
# System crash information
#------------------------------------------------------------------
System is stable and robust, don't occur crash until now!

Generate running-config..........done.

Current configuration : 914 bytes

!-----------------------------------------------------------------------
!            DXS-1210-16TC 10GbE Smart Managed Switch Configuration
!
!                            Firmware: Build V2.00.007
!         Copyright(C) 2021 D-Link Corporation. All rights reserved.
!-----------------------------------------------------------------------
command-start

!
aaa group server radius test
!
aaa new-model
aaa authentication login test radius none none none
ip http authentication aaa login-authentication test
!
line console
!
line telnet
 login authentication test
!
line ssh
 login authentication test
!
vlan 1
```

```
!
interface vlan 1
 ip address dhcp
!
interface ethernet 1/0/1
!
interface ethernet 1/0/2
!
interface ethernet 1/0/3
!
interface ethernet 1/0/4
!
interface ethernet 1/0/5
!
interface ethernet 1/0/6
#------------------------------------------------------------------------
CTRL+C ESC q Quit SPACE n Next PageENTER Next Entry a All
```

12.2. debug info

Данная команда используется для отображения информации об отладке.

debug info

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы отобразить информацию об отладке.

Пример

В данном примере показано, как отобразить информацию об отладке.

```
Switch# debug info
ARP table :
    Address     Hardware Address   Type Interface Mapping
--------------- -----------------  ---- --------- -------
192.168.0.1     14-D6-4D-39-9F-09  ARPA vlan1     Dynamic

MAC table :
 Index VLAN   MAC Address         Type    Ports
 ----  ---- ----------------    -------  -----
   1     1  14-D6-4D-39-9F-09   Dynamic    8
   2     1  E0-CB-4E-E4-3D-25   Dynamic    12

Total MAC Addresses displayed: 2
```

13. Команды DHCP Client

13.1. ip dhcp client class-id

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

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)#
```

13.2. 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. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

13.3. ip dhcp client hostname

Данная команда используется для указания значения опции имени узла (Host Name) для отправки в сообщении DHCP Discover. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

13.4. ip dhcp client lease

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

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

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)#
```

13.5. dhcp retry times

Данная команда используется для указания количества повторных попыток установки сессии DHCP. Для установки значения времени повторных попыток DHCP, заданных по умолчанию, воспользуйтесь формой **no**.

dhcp retry times *<(5-120)>*

no dhcp retry times

Параметры

<(5-120)>	Укажите количество повторных попыток установки сессии DHCP.

По умолчанию

Значение по умолчанию – 7.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для указания количества повторных попыток установки сессии DHCP.

Пример

В данном примере показано, как установить время повторных попыток DHCP.

```
Switch(config)# configure terminal
Switch(config)# dhcp retry times 10
Switch(config)#
```

13.6. show dhcp retry times

Данная команда используется для отображения количества повторных попыток установки сессии DHCP.

show dhcp retry times

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 используется для отображения количества повторных попыток установки сессии DHCP.

Пример

В данном примере показано, как отобразить время повторных попыток DHCP.

```
Switch(config)# show dhcp retry times

  DHCP Retry Times: 10
  Note: DHCP retry interval: 5 seconds

Switch(config)#
```

13.7. show ip dhcp interface

Данная команда используется для отображения параметров, связанных с DHCP, на интерфейсе.

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

Параметры

INTERFACE-ID	Укажите ID интерфейса.

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 параметров, связанных с DHCP, на интерфейсе.

Пример

В данном примере показано, как отобразить настройки, связанные с DHCP, на интерфейсе.

```
Switch(config)# show ip dhcp interface

Interface vlan1
  DHCP Client Client-ID:
  Class ID String:
  Host Name:
  Lease:


 Total Entries: 1

Switch(config)#
```

14. Команды DHCPv6 Client

14.1. show ipv6 dhcp

Данная команда используется для отображения настроек DHCPv6 на интерфейсе.

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

Параметры

INTERFACE-ID	(Опционально) Укажите интерфейс VLAN, для которого необходимо отобразить настройки DHCPv6.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

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 настройки DHCPv6 для интерфейса VLAN 1, если на VLAN 1 отключена функция DHCPv6.

```
Switch# show ipv6 dhcp interface vlan1

vlan1 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

vlan1 is in client mode
  Rapid-Commit: disabled

Switch#
```

15. Команды клиента D-Link Discovery Protocol (DDP)

15.1. ddp

Данная команда используется для того, чтобы включить функцию клиента DDP глобально или на указанных портах. Для отключения функции клиента DDP воспользуйтесь формой **no**.

ddp

no ddp

Параметры

Нет.

По умолчанию

По умолчанию данная опция включена.

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)#
```

15.2. ddp report-timer

Данная команда используется для настройки интервала между двумя последовательными сообщениями DDP Report. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

ddp report-timer {30| 60| 90|120 |Never}

no ddp report-timer

Параметры

30	Укажите, чтобы установить интервал 30 секунд.
60	Укажите, чтобы установить интервал 60 секунд.
90	Укажите, чтобы установить интервал 90 секунд.
120	Укажите, чтобы установить интервал 120 секунд.
Never	Укажите, чтобы не отправлять сообщения Report.

По умолчанию

Параметр по умолчанию – **Never**.

Режим ввода команды

Global Configuration Mode

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)#
```

15.3. 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

Любой режим конфигурирования

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 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 ethernet 1/0/1

Interface         State
--------------    ----------
eth1/0/1          Enabled

Switch#
```

16. Команды предотвращения атак DoS

16.1. dos-prevention

Данная команда используется для включения и настройки механизма предотвращения атак DoS (DoS Prevention). Для сброса значение по умолчанию для предотвращения атак DoS воспользуйтесь формой **no**.

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 к значениям по умолчанию для определенных типов атак.

Следующие распространенные типы DoS-атак могут быть обнаружены большинством коммутаторов:

- **Blat**: данный тип атаки включает в себя отправку устройству пакетов с портом источника TCP/UDP, равным порту назначения. Это может послужить причиной того, что устройство будет отвечать самому себе.
- **Land**: атака LAND включает в себя отправку устройству IP-пакетов с адресом источника и назначения, равным адресу устройства. Это может послужить причиной того, что устройство будет непрерывно отвечать самому себе.
- **TCP-NULL-scan**: сканирование порта с использованием определенных пакетов, содержащих последовательность чисел от 0 и не содержащих флаги.

- **TCP-SYN-fin**: сканирование порта с использованием определенных пакетов, содержащих флаги SYN и FIN.
- **TCP-SYN-SRCport-less-1024**: сканирование порта с использованием определенных пакетов, содержащих порт источника 0-1023 и флаг SYN.
- **TCP-xmas-scan**: сканирование порта с использованием определенных пакетов, содержащих последовательность чисел от 0 и флаги Urgent (URG), Push (PSH) и FIN.
- **Ping-death**: данный тип атаки на компьютер включает в себя отправку некорректного или вредоносного ping-запроса компьютеру. Обычно размер ping-запроса составляет 64 байта; многие компьютеры не могут распознать ping-запрос, если он больше, чем максимальный размер IP-пакета (65535 байт). Отправка ping-запроса такого размера может повредить компьютер назначения. Как правило, данным сбоем можно относительно просто воспользоваться. Отправка ping-пакета размером 65536 байт недопустима согласно сетевому протоколу, но пакет такого размера можно отправить, если он будет фрагментирован. При повторной сборке пакета буфер компьютера может переполниться, что послужит причиной сбоя системы.
- **TCP-tiny-frag**: при атаке Tiny TCP Fragment используется фрагментация IP для создания очень маленьких фрагментов, чтобы TCP-заголовок был в отдельном фрагменте пакета. Это позволяет ему обойти проверку маршрутизатора и выполнить атаку.
- **All**: все вышеперечисленные типы.

Пример

В данном примере показано, как включить механизм предотвращения атак DoS для атаки Land.

```
Switch# configure terminal
Switch(config)# dos-prevention land
Switch(config)#
```

В данном примере показано, как включить механизм предотвращения атак DoS для атак всех поддерживаемых типов.

```
Switch# configure terminal
Switch(config)# dos-prevention all
Switch(config)#
```

В данном примере показано, как отключить механизм предотвращения атак DoS для атак всех поддерживаемых типов.

```
Switch# configure terminal
Switch(config)# no dos-prevention all
Switch(config)#
```

16.2. 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

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для получения информации о статусе предотвращения атак DoS.

Пример

В данном примере показано, как отобразить информацию о настройках предотвращения атак DoS.

```
Switch# show dos-prevention

DoS Prevention Information
DoS Type                                 State
---------------------------------------- --------------
Land Attack                              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 показано, как отобразить информацию о настройках указанного типа предотвращения атак DoS.

```
Switch# show dos-prevention land

DoS Type    : Land Attack
State        : Enabled

Switch#
```

17. Команды DHCP Server Screening

17.1. based-on hardware-address

Данная команда используется для добавления записи профиля DHCP server screen. Для удаления записи воспользуйтесь формой **no**.

based-on hardware-address *CLIENT-HARDWARE-ADDRESS*

no based-on hardware-address *CLIENT-HARDWARE-ADDRESS*

Параметры

CLIENT-HARDWARE-ADDRESS	Укажите MAC-адрес клиента.

По умолчанию

Нет.

Режим ввода команды

Configure DHCP Server Screen Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Будет разрешена отправка сообщения сервера с IP-адресом указанного сервера и адресом клиента в пакете. Согласно данным записям привязок, только указанным серверам разрешено назначать адреса указанным клиентам.

Пример

В данном примере показано, как настроить профиль DHCP Server Screen «test-profile», с указанием разрешенного MAC-адреса клиента.

```
Switch# configure terminal
Switch(config)# dhcp-server-screen profile test-profile
Switch(config-dhcp-server-screen)# based-on hardware-address 00-00-00-00-00-01
Switch(config-dhcp-server-screen)#
```

17.2. clear ip dhcp snooping server-screen log

Данная команда используется, чтобы очистить буфер журнала событий Server Screen.

clear ip dhcp snooping server-screen log

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы очистить буфер журнала событий Server Screen. Буфер журнала событий DHCP Server Screen хранит информацию о пакетах, которые не прошли screening. Первый пакет, который не прошел проверку, будет отправлен в модуль журнала событий и записан в буфер журнала событий Server Screen. Последующие пакеты из той же сессии не будут отправлены в модуль журнала событий, если его запись в буфере журнала событий не будет удалена.

Пример

В данном примере показано, как очистить журнал событий Server Screen.

```
Switch# clear ip dhcp snooping server-screen log
```

17.3. dhcp-server-screen profile

Данная команда используется для настройки профиля Server Screen и входа в режим Server Screen Configure Mode. Для удаления профиля Server Screen воспользуйтесь формой **no**.

dhcp-server-screen profile *PROFILE-NAME*

no dhcp-server-screen profile *PROFILE-NAME*

Параметры

PROFILE-NAME	Укажите имя профиля. Максимальное количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы войти в режим DHCP Server Screen Configure Mode и настроить профиль Server Screen. Профиль можно использовать для настройки записи DHCP Server Screen.

Пример

В данном примере показано, как войти в режим DHCP Server Screen Configure Mode и настроить профиль «test-profile».

```
Switch# configure terminal
Switch(config)# dhcp-server-screen profile test-profile
Switch(config-dhcp-server-screen)# based-on hardware-address 00-00-00-00-00-01
Switch(config-dhcp-server-screen)#
```

17.4. ip dhcp snooping server-screen

Данная команда используется для включения DHCP Server Screening. Для отключения данной функции воспользуйтесь формой **no**.

ip dhcp snooping server-screen [*SERVER-IP-ADDRESS* **profile** *PROFILE-NAME***]**

no ip dhcp snooping server-screen *SERVER-IP-ADDRESS*

Параметры

SERVER-IP-ADDRESS	(Опционально) Укажите IP-адрес доверенного DHCP-сервера.
profile *PROFILE-NAME*	(Опционально) Укажите профиль со списком MAC-адресов клиентов для DHCP-сервера.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Функция DHCP Server Screening используется для фильтрации пакетов DHCP-сервера на указанном интерфейсе, а также для получения доверенных пакетов из указанного источника. Данная функция может сделать используемую сеть защищенной в случае, когда DHCP-Server пакеты отправляются вредоносным узлом.

Если IP-адрес сервера не указан, на интерфейсе будет включен/отключен DHCP Server Screen. По умолчанию DHCP Server Screen отключен на всех интерфейсах. Если DHCP Server Screen включен, все пакеты DHCP-сервера на указанном интерфейсе будут отфильтрованы и будут переданы только пакеты от доверенного сервера.

Если запись Server Screen определена в профиле, который содержит MAC-адрес клиента, будет передано сообщение сервера с IP-адресом сервера и адресами клиентов, содержащимися в профиле.

Если запись настроена без MAC-адреса клиента, будет передано сообщение сервера с IP-адресом указанного сервера. Каждый сервер может иметь только одну соответствующую запись в таблице.

Если запись определена в профиле, но записи не существует, сообщения с IP-адресом сервера, указанным в записи, не передаются.

Пример

В данном примере показано, как войти в профиль DHCP Server Screen «test-profile» и привязать его к Ethernet 1/0/3.

```
Switch# configure terminal
Switch(config)# dhcp-server-screen profile test-profile
Switch(config-dhcp-server-screen)# based-on hardware-address 00-00-00-00-00-01
Switch(config-dhcp-server-screen)# exit
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ip dhcp snooping server-screen 10.1.1.2 profile test-profile
Switch(config-if)#
```

17.5. ip dhcp snooping server-screen log-buffer

Данная команда используется, чтобы настроить параметр буфера журнала событий DHCP Server Screen. Для возврата к настройкам по умолчанию воспользуйтесь формой no.

ip dhcp snooping server-screen log-buffer entries *NUMBER*

no ip dhcp snooping server-screen log-buffer entries

Параметры

NUMBER	Укажите количество записей в буфере. Максимальное количество записей – 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 событий. Буфер журнала событий DHCP Server Screen хранит информацию о пакетах, которые не прошли screening. Первый пакет, который не прошел проверку, будет отправлен в модуль журнала событий и записан в буфер журнала событий Server Screen. Последующие пакеты из той же сессии не будут отправлены в модуль журнала событий, если его запись в буфере журнала не будет удалена.

Если буфер журнала событий полон, но события (нарушения) продолжают поступать, пакеты будут отброшены, а события не будут отправлены в модуль системного журнала. Если пользователь задает размер буфера меньше текущего номера записи, буфер журнала будет очищен автоматически.

Пример

В данном примере показано, как изменить размер буфера на 68.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping server-screen log-buffer entries 68
```

17.6. show ip dhcp server-screen log

Данная команда используется для отображения буфера журнала событий Server Screen.

show ip dhcp server-screen log

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить содержимое буфера журнала событий DHCP Server Screen. Буфер хранит информацию о сообщениях сервера, которые не прошли screening. Фиксируется количество нарушений одного и того же типа, а также время последнего нарушения.

Пример

В данном примере показано, как отобразить буфер журнала событий DHCP Server Screen.

```
Switch# show ip dhcp server-screen log

Total log buffer size:32

VLAN  Server IP                        Client MAC         Occurrence
----- ------------------------------- ------------------ ------------------
100    10.20.1.1                 00-20-30-40-50-60 06:30:37, 2022-02-07
100    10.58.2.30                10-22-33-44-50-60 06:31:42, 2022-02-07

Total Entries: 2
Switch#
```

17.7. snmp-server enable traps dhcp-server-screen

Данная команда используется для включения отправки SNMP-уведомлений об атаках, поступающих от ложного DHCP сервера. Для отключения отправки SNMP уведомлений воспользуйтесь формой **no**.

snmp-server enable traps dhcp-server-screen

no snmp-server enable traps dhcp-server-screen

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если после запуска функции DHCP Server Screening коммутатор получил от ложного DHCP-сервера атакующий пакет, данное событие будет занесено в журнал. Используйте данную команду, чтобы включить/отключить отправку SNMP-уведомлений о подобных событиях.

Пример

В данном примере показано, как включить отправку trap-сообщений для DHCP Server Screening.

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

18. Команды DHCP Snooping

18.1. ip dhcp snooping

Данная команда используется для глобального включения DHCP Snooping. Для отключения DHCP Snooping воспользуйтесь формой **no**.

ip dhcp snooping

no ip dhcp snooping

Параметры

Нет.

По умолчанию

По умолчанию данная функция 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 в VLAN, на которой 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 в VLAN. Таблица привязки содержит информацию о привязке IP и MAC, которая дополнительно может использоваться IP Source Guard и Dynamic ARP Inspection.

Пример

В данном примере показано, как включить DHCP Snooping.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping
Switch(config)#
```

18.2. ip dhcp snooping information option allow-untrusted

Данная команда используется для глобального доступа DHCP-пакетов с Relay Option 82 к недоверенным интерфейсам. Для запрета пакетов с Relay Option 82 воспользуйтесь формой **no**.

ip dhcp snooping information option allow-untrusted

no ip dhcp snooping information option allow-untrusted

Параметры

Нет.

По умолчанию

По умолчанию данная функция 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 которой 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)#
```

18.3. ip dhcp snooping database

Данная команда используется для настройки хранения записей привязки DHCP Snooping в локальной файловой системе (flash-памяти) или на удаленном узле. Для отключения хранения или возврата к настройкам по умолчанию воспользуйтесь формой **no**.

ip dhcp snooping database {*<tftp_url>* **| write-delay** *SECONDS***}**

no ip dhcp snooping database [write-delay]

Параметры

<tftp_url>	Укажите URL в следующем формате: • tftp://location/filename
write-delay *SECONDS*	Укажите время ожидания перед обновлением записи при обнаружении изменений в таблице привязки. Время по умолчанию составляет 300 секунд. Диапазон значений: от 60 до 86400.

По умолчанию

По умолчанию URL-адрес агента базы данных не установлен.

Значение времени задержки для записи по умолчанию составляет 300 секунд.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для хранения записей привязки DHCP на удаленном узле.

Пример

В данном примере показано, как настроить сохранение привязки в файл файловой системы.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/test
Switch(config)#
```

18.4. clear ip dhcp snooping database statistics

Данная команда используется для удаления статистики таблицы привязки DHCP.

clear ip dhcp snooping database statistics

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

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
```

18.5. clear ip dhcp snooping binding

Данная команда используется для удаления привязки DHCP.

clear ip dhcp snooping binding [*MAC-ADDR***] [***IP-ADDRESS***] [vlan** *VLAN-ID***] [interface {<***INTERFACE-ID***> | port-channel** <*1-8*>**}]**

Параметры

MAC-ADDR	(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.
port-channel <*1-8*>	(Опционально) Укажите агрегированную группу (Channel Group), которую 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
```

18.6. renew ip dhcp snooping database

Данная команда используется для обновления таблицы привязки DHCP.

renew ip dhcp snooping database *<tftp_url>*

Параметры

<tftp_url>	Укажите URL в следующем формате: • tftp://location/filename

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для обновления таблицы привязки DHCP к удаленному узлу.

Пример

В данном примере показано, как обновить таблицу привязки DHCP Snooping.

```
Switch# configure terminal
Switch(config)# renew ip dhcp snooping database tftp://10.1.1.1/test
Switch(config)#
```

18.7. ip dhcp snooping binding

Данная команда используется для настройки привязки DHCP Snooping вручную.

ip dhcp snooping binding *MAC-ADDR* **vlan** *VLAN-ID IP-ADDRESS* **interface {***<INTERFACE-ID>* **| port-channel** *<1-8>***} expiry** *SECONDS*

Параметры

MAC-ADDR	(Опционально) Укажите MAC-адрес записи, которую необходимо добавить или удалить.
IP-ADDRESS	(Опционально) Укажите IP-адрес записи, которую необходимо добавить или удалить.
vlan *VLAN-ID*	(Опционально) Укажите VLAN ID записи, которую необходимо добавить или удалить.
interface *<INTERFACE-ID>*	(Опционально) Укажите интерфейс (физический порт или port channel), на котором необходимо добавить или удалить запись привязки.
port-channel *<1-8>*	(Опционально) Укажите агрегированную группу (Channel Group) записи, которую необходимо добавить или

	удалить.
expiry *SECONDS*	Укажите интервал, по истечении которого привязки станут недействительны. 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 обновления таблицы привязки DHCP к удаленному узлу.

Пример

В данном примере показано, как настроить запись DHCP Snooping с IP-адресом 10.2.2.1 и MAC адресом 00-01-02-03-04-05 для VLAN 2 и порта Ethernet 1/0/12 с параметром expiry time, равным 100 секундам.

```
Switch# ip dhcp snooping binding 00-01-02-03-04-05 vlan 2 10.2.2.1 interface
ethernet 1/0/12 expiry 100
Switch(config)#
```

18.8. ip dhcp snooping trust

Данная команда используется для настройки порта в качестве доверенного интерфейса для DHCP Snooping. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

ip dhcp snooping trust

no dhcp snooping trust

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

Порты, подключенные к DHCP-серверу или 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, на которой включен DHCP Snooping. Коммутатор перенаправит пакеты DHCP за исключением следующих случаев, при которых пакеты будут отбрасываться:

- Порт коммутатора получает пакет (например, пакет DHCPOFFER, DHCPACK, DHCPNAK или DHCPLEASEQUERY) от DHCP-сервера за пределами межсетевого экрана.
- MAC-адрес источника в заголовке Ethernet должен быть таким же, как и аппаратный адрес DHCP-клиента, чтобы пройти проверку, если включена команда **ip dhcp snooping verify mac-address**.
- Недоверенный интерфейс получает DHCP-пакет, включающий в себя IP-адрес агента ретрансляции (Relay Agent), отличный от 0.0.0.0, или Relay Agent перенаправляет пакет, включающий в себя Option 82, на недоверенный интерфейс.
- Маршрутизатор получает сообщение DHCPRELEASE или DHCPDECLINE от недоверенного узла с записью в таблице привязки DHCP Snooping, и информация об интерфейсе в таблице привязки не соответствует интерфейсу, на котором было получено сообщение.

В дополнение к процессу проверки DHCP Snooping также создает запись 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 данном примере показано, как добавить в список доверенных интерфейсов порт 1/0/3 при использовании функции DHCP Snooping.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)#
```

18.9. ip dhcp snooping limit entries

Данная команда используется для настройки количества записей привязки DHCP Snooping, которые может изучить интерфейс. Для сброса заданного ограничения на количество записей DHCP воспользуйтесь формой **no**.

ip dhcp snooping limit entries *NUMBER*

no ip dhcp snooping limit entries

Параметры

NUMBER	Укажите номер записи привязки. Доступный диапазон значений: от 0 до 1024.

По умолчанию

По умолчанию ограничения не заданы.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима для настройки интерфейсов физического порта и port-channel. Команда действует только на недоверенных интерфейсах. Если превышено максимальное значение, система остановит изучение привязок, связанных с портом.

Пример

В данном примере показано, как установить ограничение на количество привязок для Ethernet 1/0/3. Используется значение 10.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ip dhcp snooping limit entries 10
Switch(config-if)#
```

18.10. ip dhcp snooping limit rate

Данная команда используется для настройки количества DHCP-сообщений, получаемых на интерфейсе за секунду. Для сброса заданного ограничения на получение сообщений DHCP воспользуйтесь формой **no**.

ip dhcp snooping limit rate *VALUE*

no ip dhcp snooping limit rate

Параметры

VALUE	Укажите количество DHCP-сообщений, которое может быть обработано за секунду. Доступный диапазон значений: от 0 до 300.

По умолчанию

По умолчанию ограничения не заданы.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

При превышении заданного лимита порт будет отключен из-за ошибки.

Пример

В данном примере показано, как настроить количество сообщений DHCP, которое коммутатор сможет получить на порту 1/0/3 за одну секунду.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)#
```

18.11. ip dhcp snooping station-move deny

Данная команда используется для отключения состояния DHCP Snooping Station Move. Для включения состояния DHCP Snooping Roaming воспользуйтесь формой **no**.

ip dhcp snooping station-move deny

no ip dhcp snooping station-move deny

Параметры

Нет.

По умолчанию

По умолчанию данная функция 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)#
```

18.12. ip dhcp snooping verify mac-address

Данная команда используется для включения проверки MAC-адреса источника DHCP-пакета на соответствие аппаратному адресу клиента. Для отключения проверки MAC-адреса воспользуйтесь формой **no**.

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

Параметры

Нет.

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Функция DHCP Snooping проверяет DHCP-пакеты, присылаемые на порт в VLAN, на которой включена функция DHCP Snooping. По умолчанию DHCP Snooping проверяет, совпадает ли MAC-адрес источника в заголовке Ethernet с аппаратным адресом DHCP-клиента, чтобы пройти проверку.

Пример

В данном примере показано, как включить проверку MAC-адреса источника DHCP-пакета и аппаратного адреса клиента.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping verify mac-address
Switch(config)#
```

18.13. ip dhcp snooping vlan

Данная команда используется для включения DHCP Snooping в определенной VLAN или группе VLAN. Для отключения DHCP Snooping в VLAN или группе VLAN воспользуйтесь формой **no**.

ip dhcp snooping vlan *VLAN-ID* **[, | -]**

no ip dhcp snooping vlan *VLAN-ID* **[, | -]**

Параметры

VLAN-ID	Укажите VLAN ID, которые защищены механизмом ERP. 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 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 в VLAN, на которой включена функция DHCP Snooping. С помощью данной функции DHCP-пакеты, приходящие с недоверенного интерфейса, могут получить статус проверенных, а для VLAN с включенной функцией DHCP Snooping будет создана таблица привязки DHCP. Таблица привязки предоставляет информацию о соответствиях IP- и MAC-адресов, которая позже может использоваться функциями IP Source Guard и Dynamic ARP Inspection.

Пример

В данном примере показано, как включить DHCP Snooping в VLAN 10.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping vlan 10
Switch(config)#
```

18.14. show ip dhcp snooping

Данная команда используется для отображения настроек DHCP Snooping.

show ip dhcp snooping

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения настроек DHCP Snooping.

Пример

В данном примере показано, как получить информацию по настройкам DHCP Snooping.

```
Switch# show ip dhcp snooping

DHCP Snooping is enabled
DHCP Snooping is enabled on VLANs:

Verification of MAC address is enabled
Information option of allowed on un-trusted interface is disabled
Station Move Deny is disabled

Interface      Trusted   Rate Limit  Entry Limit
-------------- --------- ----------- -----------
eth1/0/1       yes       no_limit    10
eth1/0/2       yes       no_limit    no_limit
eth1/0/3       yes       no_limit    no_limit
eth1/0/4       yes       no_limit    no_limit
eth1/0/5       yes       no_limit    no_limit
eth1/0/6       yes       no_limit    no_limit
eth1/0/7       yes       no_limit    no_limit
eth1/0/8       yes       no_limit    no_limit
eth1/0/9       yes       no_limit    no_limit
eth1/0/10      yes       no_limit    no_limit
eth1/0/11      yes       no_limit    no_limit
eth1/0/12      yes       no_limit    no_limit
eth1/0/13      yes       no_limit    no_limit
eth1/0/14      yes       no_limit    no_limit
eth1/0/15      yes       no_limit    no_limit
eth1/0/16      yes       no_limit    no_limit
```

19. Команды Error Recovery

19.1. errdisable recovery

Данная команда используется для включения функции Error Recovery (восстановление ошибок), а также для настройки Recovery Interval (время восстановления). Для отключения опции Auto-Recovery или возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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} [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 в секундах, необходимое для восстановления порта при ошибке, вызванной указанным модулем. Доступный диапазон значений: от 5 до 86400 секунд. Значение по умолчанию – 300 секунд.

По умолчанию

По умолчанию опция Auto-Recovery отключена для всех ситуаций.

Режим ввода команды

Global Configuration Mode

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 действовать опция no shutdown.

Восстановить порт при возникновении ошибки можно двумя способами. При помощи команды **errdisable recovery cause** администратор может включить функцию Auto-Recovery на портах, отключенных при возникновении конкретных ошибок. Также порт можно восстановить вручную, для этого сначала введите команду **shutdown**, а затем **no shutdown**.

Пример

В данном примере показано, как установить Recovery Timer (таймер восстановления) на 200 секунд для восстановления порта при ошибке, вызванной Port Security Violation.

```
Switch# configure terminal
Switch(config)#errdisable recovery cause psecure-violation interval 200
Switch(config)#
```

В данном примере показано, как включить опцию Auto-Recovery для восстановления порта при ошибке, вызванной Port Security Violation.

```
Switch# configure terminal
Switch(config)#errdisable recovery cause psecurity-violation
Switch(config)#
```

19.2. 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

Любой режим конфигурирования

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(config)#show errdisable recovery

ErrDisable Cause         State        Interval
-----------------------  ----------   ------------
Port Security            disabled     120 seconds
Storm Control            disabled     120 seconds
ARP Rate                 disabled     120 seconds
BPDU Attack Protection   disabled     120 seconds
DHCP Rate                disabled     120 seconds
Loopback Detect          enabled      120 seconds

Interfaces that will be recovered at the next timeout:
Interface    vlan    ErrDisable Cause         Time left
----------   ------  -----------------------   ------------
ethernet 1/0/1     -       Loopback Detect          105 seconds
ethernet 1/0/2     -       Loopback Detect          105 seconds

Switch#
```

19.3. snmp-server enable traps errdisable

Данная команда используется для того, чтобы включить отправку SNMP-уведомлений об ошибке на порту. Для отключения отправки уведомлений воспользуйтесь формой **no**.

snmp-server enable traps errdisable [asserted] [cleared] [notification-rate *TRAP-RATE***]**

no snmp-server enable traps errdisable [asserted] [cleared] [notification-rate]

Параметры

asserted	(Опционально) Укажите, чтобы отправлять уведомления при возникновении ошибки на порту.
cleared	(Опционально) Укажите, чтобы отправлять уведомления при устранении ошибки на порту.
notification-rate *TRAP-RATE*	(Опционально) Укажите, чтобы настроить количество трапов в минуту. Доступный диапазон значений: от 0 до 1000. Пакеты, превышающие указанное значение, будут отброшены. Если указан 0, то SNMP-уведомления будут генерироваться при каждом изменении ошибки на порту.

По умолчанию

По умолчанию все типы уведомлений отключены и количество уведомлений не ограничено.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда с параметрами **asserted** и **cleared** включает или отключает уведомления об изменении ошибки на порту. При вводе команды с одним из параметров, будет включен или отключен только указанный тип уведомления. Состояние или значение другого типа уведомления не будут изменены.

Команды **snmp-server enable traps errdisable notification-rate** и **no snmp-server enable traps errdisable notification-rate** влияют только на настройку количества уведомлений в минуту, а не на состояние отправки уведомлений об ошибке на порту.

Пример

В данном примере показано, как включить отправку трапов при возникновении и устранении ошибки на порту, а также установить максимальное количество трапов в минуту равным 3.

```
Switch# configure terminal
Switch(config)#snmp-server enable traps errdisable asserted cleared notification-
rate 3
Switch(config)#
```

19.4. show snmp-server traps error-disable

Данная команда используется для отображения SNMP-уведомлений об ошибке на порту.

show snmp-server traps error-disable

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки SNMP-уведомлений об ошибке на порту.

Пример

В данном примере показано, как отобразить настройки SNMP-уведомлений об ошибке на порту.

```
Switch# show snmp-server traps error-disable

Error Disable Trap:
    Asserted: disabled
    Cleared: disabled
    Notification Rate: 0
```

20. Команды Ethernet Ring Protection Switching (ERPS)

Для получения дополнительной информации см. **Приложение E – Информация ERPS**.

20.1. description

Данная команда используется для настройки описания экземпляров Ethernet Ring Protection Switching (ERPS).

description *DESCRIPTION*

no description *DESCRIPTION*

Параметры

DESCRIPTION	Укажите описание экземпляров Ethernet Ring Protection (ERPS).

По умолчанию

Нет.

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для настройки описания экземпляров ERPS.

Пример

В данном примере показано, как настроить описание для экземпляров ERPS.

```
Switch#configure terminal
Switch(config)# erps instance 1
Switch(config-erp-instance)#description custom-description
Switch(config-erp-instance)#
```

20.2. ring

Данная команда используется для создания или изменения физического кольца ERPS ITU-T G.8032 и перехода в режим ERPS Configuration Mode. Для удаления указанного кольца воспользуйтесь формой **no**.

ring *RING-NAME*

no ring *RING -NAME*

Параметры

RING-NAME	Укажите имя кольца ERPS. Максимально допустимое количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для создания, изменения или удаления физического кольца ERPS ITU-T G.8032 и перехода в режим ERPS Configuration Mode.

Пример

В данном примере показано, как создать кольцо ERPS «campus».

```
Switch#configure terminal
Switch(config)# erps instance 1
Switch(config-erps-instance)#ring campus
```

20.3. ethernet ring g8032 profile

Данная команда используется для создания или изменения профиля G.8032 и входа в режим ERPS Configuration Mode. Для удаления указанного профиля воспользуйтесь формой **no**.

erps profile *PROFILE-NAME*

no erps 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

Данная команда используется для создания, изменения или удаления профиля G.8032 и входа в режим ERPS Configuration Mode.

Пример

В данном примере показано, как создать профиль G.8032 «campus».

```
Switch#configure terminal
Switch(config)# erps profile campus
Switch (config-erps-profile)#
```

20.4. r-aps channel-vlan

Данная команда используется для настройки ERPS R-APS VLAN. Для удаления настройки воспользуйтесь формой **no**.

r-aps channel-vlan *VLAN-ID*

no r-aps channel-vlan

Параметры

VLAN-ID	Укажите VLAN ID. 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

Данная команда используется для назначения R-APS VLAN для экземпляра ERPS. Создать и назначить R-APS VLAN необходимо до того, как для экземпляра ERPS будет включен рабочий режим.

Указанная R-APS VLAN не обязательно должна существовать для настройки команды. Но она должна существовать, прежде чем экземпляр будет переведен в рабочий режим.

Если R-APS VLAN удалена во время работы экземпляра ERPS, экземпляр ERPS перейдет в отключенный рабочий режим.

У каждого экземпляра ERPS должна быть отдельная R-APS VLAN.

Пример

В данном примере показано, как настроить R-APS VLAN 2 для ERPS-экземпляра 1.

```
Switch(config)# erps instance 1
Switch(config-erp-instance)#r-aps channel-vlan 2
Switch(config-erp-instance)#
```

20.5. inclusion-list vlan-ids

Данная команда используется для настройки заданных VLAN ID, которые защищены механизмом Ethernet Ring Protection. Для удаления VLAN ID воспользуйтесь формой **no**.

inclusion-list vlan-ids *VLAN-ID* **[, | -]**

no inclusion-list vlan-ids *VLAN-ID* **[, | -]**

Параметры

VLAN-ID	Укажите VLAN ID, которые защищены механизмом 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

Данная команда используется для добавления или удаления нескольких VLAN ID, которые защищены механизмом ERPS.

Пример

В данном примере показано, как сконфигурировать защищенные сервисом Ethernet Ring Protection VLAN 100-200 для ERPS-экземпляра 1.

```
Switch#configure terminal
Switch(config)# erps instance 1
Switch(config-erp-instance)#inclusion-list vlan-ids 100-200
Switch(config-erp-instance)#
```

20.6. instance

Данная команда используется для создания экземпляра ERPS и входа в режим ERPS Instance Configuration Mode. Для удаления экземпляра ERPS воспользуйтесь формой **no**.

erps instance *INSTANCE-ID*

no erps instance *INSTANCE-ID*

Параметры

INSTANCE-ID	Укажите номер экземпляра ERPS. Доступный диапазон значений: от 1 до 32.

По умолчанию

Нет.

Режим ввода команды

ERPS Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для создания или удаления экземпляра ERPS и входа в режим ERPS Instance Configuration Mode.

Пример

В данном примере показано, как создать ERPS-экземпляр 1 в физическом кольце «ring2».

```
Switch#configure terminal
Switch(config)# erps instance 1
Switch(config-erp-instance)#
```

20.7. level

Данная команда используется для настройки значения MEL кольца экземпляра ERPS. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

level *MEL-VALUE*

no level

Параметры

MEL-VALUE	Укажите значение MEL кольца экземпляра ERPS. Доступный диапазон значений: 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

Данная команда используется для настройки значения MEL кольца экземпляра ERPS. Значение MEL кольца всех узлов в одном экземпляре ERPS должно быть идентичным.

Пример

В данном примере показано, как настроить значение MEL кольца ERPS-экземпляра 1. Указанное значение – 6.

```
Switch#configure terminal
Switch(config)# erps instance 1
Switch(config-erp-instance)#level 6
Switch(config-erp-instance)#
```

20.8. profile

Данная команда используется для привязки экземпляра ERPS к профилю G.8032. Для удаления привязки воспользуйтесь формой **no**.

profile *PROFILE-NAME*

Параметры

PROFILE-NAME	Укажите имя профиля, к которому необходимо привязать экземпляр ERPS.

По умолчанию

Нет.

Режим ввода команды

ERPS Instance Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для привязки экземпляра ERPS к профилю G.8032. Несколько экземпляров ERPS могут быть привязаны к одному и тому же профилю G.8032. Экземпляры, связанные с одним и тем же профилем, защищают один и тот же набор VLAN, или VLAN, защищенные одним экземпляром, являются подмножеством локальных сетей, защищенных другим экземпляром.

Пример

В данном примере показано, как привязать профиль «campus» к экземпляру 1.

```
Switch#configure terminal
Switch(config)# erps instance 1
Switch(config-erp-instance)#profile campus
Switch(config-erp-instance)#
```

20.9. port0

Данная команда используется для указания первого порта физического кольца. Для удаления заданных настроек воспользуйтесь формой **no**.

port0 interface {*INTERFACE-ID* **| port-channel** <*1-8*>**}**

no port0 interface {*INTERFACE-ID* **| port-channel** <*1-8*>**}**

Параметры

INTERFACE-ID	Укажите interface ID первого порта кольца.
port-channel	Укажите агрегированную группу (Channel Group) первого порта кольца.

По умолчанию

Нет.

Режим ввода команды

ERPS Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для указания или удаления первого порта физического кольца.

Пример

В данном примере показано, как настроить порт Ethernet 1/0/1 в качестве первого порта кольца G.8032 «ring1».

```
Switch#configure terminal
Switch(config)# erps instance 1
Switch(config-erps-instance)# port0 interface ethernet 1/0/1
Switch(config-erps-instance)#
```

20.10. port1

Данная команда используется для указания второго порта физического кольца. Для удаления заданных настроек воспользуйтесь формой **no**.

port1 {interface *INTERFACE-ID* **}**

Параметры

INTERFACE-ID	Укажите второй порт кольца. Доступны физические порты и port-channel.

По умолчанию

Нет.

Режим ввода команды

ERPS Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для указания или удаления второго порта физического кольца.

Пример

В данном примере показано, как настроить связанный узел в качестве конечного локального узла кольца G.8032 «ring2».

```
Switch#configure terminal
Switch(config)# erps instance 1
Switch(config-erps-instance)# port1 interface ethernet 1/0/1
Switch(config-erps-instance)#
```

20.11. revertive

Данная команда используется для возврата к действующему средству передачи, например, когда RPL был заблокирован. Для того чтобы продолжить использование RPL, при условии его исправности, после устранения ошибки на коммутаторе воспользуйтесь формой **no**.

revertive

no revertive

Параметры

Нет.

По умолчанию

Параметр по умолчанию – **revertive**.

Режим ввода команды

G.8032 Profile Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

После того, как неисправность коммутатора устранена, канал трафика будет восстанавливаться по истечении времени WTR Timer, который используется для предотвращения частого переключения порта, если соединение на каком-то участке кольца очень часто меняет состояние.

Если нереверсивный режим выключен, после устранения ошибки канал трафика продолжает использовать RPL при условии его исправности. С учетом защиты Ethernet-кольца ресурсы действующих средств передачи могут быть оптимизированы, в некоторых случаях рекомендуется вернуться к действующему средству передачи, как только будут доступны все кольцевые соединения. Это выполняется за счет дополнительного разрыва соединения. В некоторых случаях нет преимуществ в немедленном возврате к действующим средствам передачи данных. При этом можно избежать второго разрыва, если не восстанавливать защитное переключение.

Пример

В данном примере показано, как включить нереверсивный режим для колец профиля «campus».

```
Switch#configure terminal
Switch(config)# erps profile campus
Switch (config-erps-profile)# no revertive
Switch (config-erps-profile)#
```

20.12. rpl

Данная команда используется для настройки узла в качестве RPL Owner или для назначения порта RPL. Для удаления настроек RPL воспользуйтесь формой **no**.

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.

По умолчанию

Нет.

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для настройки узла в качестве RPL Owner или RPL Neighbor, а также для назначения порта RPL.

Пример

В данном примере показано, как настроить порт 0 в качестве порта RPL ERPS экземпляра 1.

```
Switch#configure terminal
Switch(config)# erps instance 1
Switch(config-erp-instance)#rpl port0
Switch(config-erp-instance)#
```

20.13. show ethernet ring g8032

Данная команда используется для отображения информации об экземплярах ERPS.

show ethernet ring g8032 {status | brief}

Параметры

status	Укажите, чтобы отобразить статус экземпляров ERPS.
brief	Укажите, чтобы отобразить краткую информацию об экземплярах ERPS.

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 об экземплярах ERPS.

Пример

В данном примере показано, как отобразить подробную информацию об ERPS.

```
Switch#show ethernet ring g8032 status

 Ethernet ring ring2,instance 0
 ---------------------------------------
     Description:
     MEL: 1
     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: -
     Admin Port0: ethernet 1/0/1
     Operational Port0: ethernet 1/0/1
     Port0 State: Forwarding
     Admin Port1: ethernet 1/0/2
     Operational Port1: ethernet 1/0/2
     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 данном примере показано, как отобразить краткую информацию об экземплярах ERPS.

```
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:ethernet 1/0/1,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/No TC Propagation	TC распространяются / не распространяются в кольце.
Revertive / Non-Revertive	Реверсивный / нереверсивный режим работы колец.
Instance State	Текущий статус узла кольца экземпляра ERPS. (Deactivated / Init / Idle / Protection)
Admin/Operational RPL	Текущая роль узла экземпляра ERPS. (Owner / None).
Admin/Operational Port0/port1	Текущая роль кольцевого порта. (Interface_id / None).
Admin/Operational RPL Port	Текущие настройки RPL. (Port0 / Port1 / None).
Ring port0/port1 state	Статус кольцевых портов экземпляра ERPS. (- / Forwarding / Blocked l).

Profile	Профиль, привязанный к экземплярам кольца.
Inst ID	Идентификатор экземпляра ERPS.
RingType	Тип кольца (основное кольцо / подкольцо).
Node Type	RPL Owner.
Status	Текущий статус экземпляра ERPS. Это может быть одно из следующих значений: **Deactivated:** экземпляр ERPS деактивирован. **Init:** экземпляр инициализируется. **Idle:** экземпляр находится в нормальном состоянии. Порт RPL заблокирован. **Protection:** экземпляр обнаруживает сбой на каком-то кольцевом порту. Порт RPL восстанавливается для защиты порта.
Port-State	Текущий статус кольцевых портов. (- / Forwarding / Blocked).

20.14. activate

Данная команда используется для включения указанного экземпляра ERPS. Для отключения указанного экземпляра ERPS воспользуйтесь формой **no**.

activate

no activate

Параметры

Нет.

По умолчанию

Параметр по умолчанию – **no activate**.

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для включения или отключения указанного экземпляра ERPS. Перед этим необходимо настроить кольцевые порты, R-APS и профиль ERPS.

Включенный экземпляр ERPS будет находиться в нерабочем состоянии, если указанный R-APS не существует или указанные порты не являются тегированным членом порта R-APS VLAN.

Пример

В данном примере показано, как включить экземпляр 1.

```
Switch#configure terminal
Switch(config)# erps instance 1
Switch(config-erp-instance)#activate
Switch(config-erp-instance)#
```

20.15. timer

Данная команда используется для того, чтобы настроить таймеры для домена ERPS. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

timer {guard *MILLI-SECONDS* **| hold-off** *SECONDS* **| wtr** *MINUTES***}**

no timer {guard | hold-off | wtr}

Параметры

guard *MILLI-SECONDS*	(Опционально) Укажите значение Guard Timer в диапазоне от 10 до 2000 миллисекунд.
hold-off *SECONDS*	(Опционально) Укажите значение Hold-Off Timer в диапазоне от 0 до 10 секунд.
wtr *MINUTES*	(Опционально) 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

Данная команда используется для того, чтобы настроить таймеры для домена ERPS.

Пример

В данном примере показано, как настроить Guard Timer со значением 700 миллисекунд для профиля «campus».

```
Switch#configure terminal
Switch(config)# erps profile campus
Switch (config-erps-profile)# timer guard 700
```

21. Команды Filter Database (FDB)

21.1. 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#
```

21.2. mac-address-table aging-time

Данная команда используется для настройки времени устаревания MAC-адресов в таблице. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

21.3. mac-address-table aging destination-hit

Данная команда используется для включения функции Destination MAC Address Triggered Update. Для отключения данной функции воспользуйтесь формой **no**.

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)#
```

21.4. mac-address-table learning

Данная команда используется для включения изучения MAC-адресов на физическом порту. Для отключения данной функции воспользуйтесь формой **no**.

mac-address-table learning interface *INTERFACE-ID* **[, | -]**

no mac-address-table learning interface *INTERFACE-ID* **[, | -]**

Параметры

INTERFACE-ID	(Опционально) 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 данную команду, чтобы включить/отключить изучение MAC-адресов на физическом порту.

Пример

В данном примере показано, как включить опцию изучения MAC-адресов.

```
Switch# configure terminal
Switch(config)#mac-address-table learning interface ethernet 1/0/5
Switch(config)#
```

21.5. mac-address-table static

Данная команда используется для добавления статического адреса в таблицу MAC-адресов. Для удаления записи из таблицы воспользуйтесь формой **no**.

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 данном примере показано, как добавить статический адрес C2:F3:22:0A:12:F4 в таблицу MAC-адресов. Если пакет с MAC-адресом назначения C2:F3:22:0A:12:F4 получен на VLAN 4, он будет направлен на интерфейс Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)#mac-address-table static C2:F3:22:0A:12:F4 vlan 4 interface ethernet 1/0/1
Switch(config)#
```

В данном примере показано, как добавить статический адрес C2:F3:22:0A:22:33 в таблицу MAC-адресов. Если пакет с MAC-адресом назначения C2:F3:22:0A:22:33 получен на VLAN 4, он будет направлен на port-channel 2.

```
Switch# configure terminal
Switch(config)#interface range ethernet 1/0/5-6
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-channel2
Switch(config)#
```

21.6. multicast filtering-mode

Данная команда используется для настройки способа обработки групповых пакетов для VLAN. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

multicast filtering-mode {forward-all | forward-unregistered | filter-unregistered}

no multicast filtering-mode

Параметры

forward-all	Укажите, чтобы распространить все групповые пакеты на основании VLAN-домена.
forward-unregistered	Укажите, чтобы направить зарегистрированные групповые пакеты на основании таблицы переадресации и распространить все незарегистрированные групповые пакеты на основании VLAN-домена.
filter-unregistered	Укажите, чтобы направить зарегистрированные пакеты на основании таблицы переадресации и отфильтровать все незарегистрированные групповые пакеты.

По умолчанию

Параметр по умолчанию – **forward-unregistered**.

Режим ввода команды

VLAN Configuration Mode

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)#
```

21.7. show mac-address-table

Данная команда используется для отображения записи указанного MAC-адреса или записей MAC-адреса для указанного интерфейса/VLAN.

show mac-address-table [dynamic | static] [address *MAC-ADDR* **| interface** *INTERFACE-ID* **| vlan** *VLAN-ID***]**

Параметры

dynamic	(Опционально) Укажите, чтобы отобразить только записи

	таблицы динамических MAC-адресов.
static	(Опционально) Укажите, чтобы отобразить только записи таблицы статических MAC-адресов.
address *MAC-ADDR*	(Опционально) Укажите 48-битный MAC-адрес.
interface *INTERFACE-ID*	(Опционально) Укажите, чтобы отобразить информацию для указанного интерфейса (физического порта или port-channel).
vlan *VLAN-ID*	(Опционально) Укажите VLAN ID в диапазоне от 1 до 4094.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

При указании параметра **interface** будет отображена индивидуальная запись, чей интерфейс передачи соответствует указанному интерфейсу.

Пример

В данном примере показано, как отобразить все записи таблицы MAC-адресов для MAC-адреса 00-02-4b-28-c4-82.

```
Switch# show mac-address-table address 00:02:4B:28:C4:82

VLAN    MAC Address        Type    Ports
------ ----------------- -------- --------
1      00-02-4B-28-C4-82   Dynamic  ethernet 1/0/1

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
----------------------------------------
4     00-01-00-02-00-04     Static    ethernet 1/0/2
4     C2-F3-22-0A-12-F4     Static    port-channel2
6     00-01-00-02-00-07     Static    ethernet 1/0/1
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     00-03-40-11-22-33    Dynamic        ethernet 1/0/2

Total Entries: 2

Switch#
```

21.8. show mac-address-table aging-time

Данная команда используется для отображения времени устаревания MAC-адресов в таблице.

show mac-address-table aging-time

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

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.
Aging Destination Hit is disabled.

Switch#
```

21.9. show mac-address-table learning

Данная команда используется для отображения статуса изучения MAC-адресов.

show mac-address-table learning [interface *INTERFACE-ID* **[, | -]]**

Параметры

INTERFACE-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

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если интерфейс не указан, будут отображены все существующие интерфейсы.

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
-------------------------   --------
ethernet 1/0/1                    Enabled
ethernet 1/0/2                    Enabled
ethernet 1/0/3                    Enabled
ethernet 1/0/4                    Enabled
ethernet 1/0/5                    Enabled
ethernet 1/0/6                    Enabled
ethernet 1/0/7                    Enabled
ethernet 1/0/8                    Enabled
ethernet 1/0/9                    Enabled
ethernet 1/0/10                   Enabled

Switch#
```

21.10. show multicast filtering-mode

Данная команда используется для отображения режима фильтрации при обработке групповых пакетов, полученных на интерфейсе.

show multicast filtering-mode [interface *VLAN-ID***]**

Параметры

interface *VLAN-ID*	(Опционально) Укажите VLAN, которую необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

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#
```

22. Команды GARP VLAN Registration Protocol (GVRP)

22.1. clear gvrp statistics

Данная команда используется для удаления статистики GVRP на порту.

clear gvrp statistics {all | interface *INTERFACE-ID* **[, | -] | port-channel** *<1-8>***}**

Параметры

all	Укажите, чтобы обнулить счетчики статистики GVRP, ассоциированные со всеми интерфейсами.
INTERFACE-ID	Укажите интерфейс физического порта.
,	(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.
port-channel *<1-8>*	Укажите агрегированную группу (Channel Group) для сброса счетчика.

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#
```

22.2. gvrp global

Данная команда используется для глобального включения функции GVRP. Для глобального отключения функции GVRP воспользуйтесь формой **no**.

gvrp global

no gvrp global

Параметры

Нет.

По умолчанию

По умолчанию данная функция 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)#
```

22.3. gvrp enable

Данная команда используется для включения функции GVRP на порту. Для отключения функции воспользуйтесь формой **no**.

gvrp enable

no gvrp 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 применима исключительно для настройки интерфейсов физического порта и port-channel в режимах hybrid и trunk. Если для GVRP включена функция Layer 2 Protocol Tunnel, применение команды невозможно.

Пример

В данном примере показано, как включить функцию GVRP на интерфейсе Ethernet 1/0/4.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/4
Switch(config-if)# gvrp enable
Switch(config-if)#
```

22.4. gvrp advertise

Данная команда позволяет указать VLAN, для которых разрешено анонсирование при помощи GVRP-протокола. Для отключения данной функции воспользуйтесь формой **no**.

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. 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 применима исключительно для настройки интерфейсов физического порта и port-channel в режимах hybrid и trunk. 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 порту Ethernet 1/0/4.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/4
Switch(config-if)# gvrp advertise 1000
Switch(config-if)#
```

22.5. gvrp vlan create

Данная команда используется, чтобы включить создание Dynamic VLAN. Для отключения функции воспользуйтесь формой **no**.

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. В противном случае 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)#
```

22.6. gvrp forbidden

Данная команда используется для указания порта, которому запрещено быть членом обозначенной VLAN. Для удаления статуса запрещенного члена всех VLAN для порта воспользуйтесь формой **no**.

gvrp forbidden {all | [add | remove] *VLAN-ID* **[, | -]}**

no gvrp forbidden

Параметры

all	Укажите, чтобы запретить на интерфейсе все VLAN.
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 VLAN ID, который необходимо добавить в список запрещенных VLAN или удалить из данного списка. Если не указан параметр **add** или **remove**, список данных VLAN заменит текущий список запрещенных VLAN. 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 ни одна из VLAN не запрещена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и port-channel в режимах hybrid и trunk. 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 необходимо предварительно включить GVRP.

Пример

В данном примере показано, как настроить порт Ethernet 1/0/4 как запрещенный порт для VLAN 100 при помощи GVRP.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/4
Switch(config-if)# gvrp forbidden 100
Switch(config-if)#
```

22.7. gvrp timer

Данная команда используется, чтобы настроить значение таймера GVRP на порту. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

gvrp timer [join *TIMER-VALUE***] [leave** *TIMER-VALUE***] [leave-all** *TIMER-VALUE***]**

no gvrp timer [join] [leave] [leave-all]

Параметры

join *TIMER-VALUE*	(Опционально) Установите значение таймера для входа в группу. Единицы измерения – сотые доли секунды. Доступный диапазон значений: от 10 до 10000.
leave *TIMER-VALUE*	(Опционально) Установите значение таймера для выхода из группы. Единицы измерения – сотые доли секунды. Доступный диапазон значений: от 10 до 10000.
leave-all *TIMER-VALUE*	Установите значение таймера для выхода из всех групп. Единицы измерения – сотые доли секунды.

По умолчанию

Join: 20.

Leave: 60.

Leave-all: 1000.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется, чтобы установить 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)#
```

22.8. show gvrp configuration

Данная команда используется для отображения настроек GVRP.

show gvrp configuration {interface *INTERFACE-ID* **[, | -] | port-channel** <*1-8*>**}**

Параметры

INTERFACE-ID	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.
port-channel <*1-8*>	Укажите агрегированную группу (Channel Group) для сброса счетчика.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения настроек GVRP. Если параметр не указан, будут отображены глобальные настройки GVRP.

Пример

В данном примере показано, как отобразить глобальные настройки GVRP.

```
Switch(config-if)# show gvrp configuration interface ethernet 1/0/4

eth1/0/4
 GVRP Status:     Enabled
 Join Time:       20              centiseconds
 Leave Time:      60              centiseconds
 Leave-All Time:  1000            centiseconds
 Advertise VLAN:
 Forbidden VLAN:  100
Switch(config-if)#
```

22.9. show gvrp statistics

Данная команда используется для отображения статистики GVRP на порту.

show gvrp statistics [interface *INTERFACE-ID* **[, | -] | port-channel** <*1-8*>**]**

Параметры

INTERFACE-ID	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.
port-channel <*1-8*>	Укажите агрегированную группу (Channel Group) для сброса счетчика.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда позволяет отобразить порты, на которых включен режим GVRP.

Пример

В данном примере показано, как отобразить статистику GVRP для интерфейса Ethernet 1/0/4.

```
Switch# show gvrp statistics interface ethernet 1/0/4
 Interface       JoinEmpty  JoinIn     LeaveEmpty LeaveIn    LeaveAll   Empty

---------------------------------------------------------------------------
 eth1/0/4      RX 0          0          0          0          0          0

               TX 0          0          0          0          0          0

Switch#
```

23. Команды IGMP Snooping

23.1. clear ip igmp snooping statistics

Данная команда используется для удаления статистики IGMP Snooping.

clear ip igmp snooping statistics {all | vlan *VLAN-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.

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#
```

23.2. ip igmp snooping

Данная команда используется для включения функции IGMP Snooping на коммутаторе. Для отключения данной функции воспользуйтесь формой **no**.

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

Interface 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 глобально.

```
Switch# configure terminal
Switch(config)#no ip igmp snooping
Switch(config)#
```

В данном примере показано, как включить функцию IGMP Snooping глобально.

```
Switch# configure terminal
Switch(config)# ip igmp snooping
Switch(config)#
```

В данном примере показано, как отключить функцию IGMP Snooping на VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# no ip igmp snooping
Switch(config-vlan)#
```

23.3. ip igmp snooping fast-leave

Данная команда используется для настройки функции IGMP Snooping Fast Leave на интерфейсе. Для отключения данной функции на указанном интерфейсе воспользуйтесь формой **no**.

ip igmp snooping fast-leave

no ip igmp snooping fast-leave

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 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)#
```

23.4. ip igmp snooping last-member-query-interval

Данная команда используется для настройки интервала, в течение которого IGMP Snooping Querier отправляет сообщения Group-Specific Query (с указанием группы) или Group-Source-Specific Query (с указанием источника группы) / Channel-Source-Specific Query (с указанием источника канала). Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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

Interface 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)#
```

23.5. ip igmp snooping mrouter

Данная команда используется для настройки указанного интерфейса/интерфейсов в качестве multicast router-портов, а также для указания интерфейса/интерфейсов, которые не могут быть multicast router-портами. Для удаления интерфейса/интерфейсов из списка router-портов или списка запрещенных router-портов воспользуйтесь формой **no**.

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	(Опционально) Укажите интерфейс или список интерфейсов. В качестве интерфейса может быть использован физический порт или port-channel.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса

недопустимы.

По умолчанию

По умолчанию multicast router-порты IGMP Snooping отсутствуют.

По умолчанию включено автоматическое изучение.

Режим ввода команды

Interface 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.

Пример

В данном примере показано, как добавить статический multicast router-порт IGMP Snooping для VLAN 1.

```
Switch# configure terminal
Switch(config)#vlan 1
Switch(config-vlan)# ip igmp snooping mrouter interface eth 1/0/1
Switch(config-vlan)#
```

23.6. ip igmp snooping querier

Данная команда используется для указания устройства в качестве IGMP Snooping Querier. Для отключения данной функции воспользуйтесь формой **no**.

ip igmp snooping querier

no ip igmp snooping querier

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 может применяться только для настройки интерфейса VLAN. Если система может выполнить роль Querier, устройство будет ожидать пакеты IGMP Query, отправленные другими устройствами. При получении сообщения IGMP Query устройство с более низким значением IP-адреса становится Querier.

Пример

В данном примере показано, как включить IGMP Snooping Querier на VLAN 1.

```
Switch# configure terminal
Switch(config)#vlan 1
Switch(config-vlan)# ip igmp snooping querier
Switch(config-vlan)#
```

23.7. ip igmp snooping query-interval

Данная команда используется для настройки интервала между сообщениями IGMP General Query. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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

Interface 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)#
```

23.8. ip igmp snooping query-max-response-time

Данная команда используется для настройки максимального значения времени ожидания, анонсированного в сообщениях IGMP Snooping Query. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

ip igmp snooping query-max-response-time *SECONDS*

no ip igmp snooping query-max-response-times

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

Interface 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 VLAN 1000. Указанное значение – 20 секунд.

```
Switch# configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)# ip igmp snooping query-max-response-time 20
Switch(config-vlan)#
```

23.9. ip igmp snooping query-version

Данная команда используется для настройки версии пакетов General Query, отправляемых IGMP Snooping Querier. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

ip igmp snooping query-version {1 | 2 | 3}

no ip igmp snooping query-version

Параметры

NUMBER	Укажите версию пакета IGMP General Query, отправленного IGMP Snooping Querier.

По умолчанию

Значение по умолчанию – 3.

Режим ввода команды

Interface 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)#
```

23.10. ip igmp snooping robustness-variable

Данная команда используется для настройки robustness variable (переменной надежности), используемой в IGMP Snooping. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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

Interface 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 многоадресный 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)#
```

23.11. ip igmp snooping static-group

Данная команда используется для настройки статической группы IGMP Snooping. Для удаления статической группы воспользуйтесь формой **no**.

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-ID	(Опционально) 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

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Используйте данную команду на интерфейсе VLAN, чтобы добавить запись статической группы.

Используйте команду **ip igmp snooping static-group**, чтобы создать статическую группу IGMP Snooping, если подключенный узел не поддерживает IGMP-протокол.

Пример

В данном примере показано, как добавить запись статической группы для IGMP Snooping.

```
Switch# configure terminal
Switch(config)#vlan 1
Switch(config-vlan)# ip igmp snooping static-group 226.1.2.3 interface ethernet
1/0/5
Switch(config-vlan)#
```

23.12. 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

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию об IGMP Snooping для всех VLAN, на которых включена данная функция.

Пример

В данном примере показано, как отобразить общее состояние IGMP Snooping.

```
Switch#show ip igmp snooping

IGMP snooping global state: Enabled

Switch#
```

В данном примере показано, как отобразить информацию об IGMP Snooping на VLAN 2.

```
Switch#show ip igmp snooping vlan 2

    IGMP snooping state              : Disabled
    Fast leave                       : Enabled (host-based)
    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

Switch#
```

23.13. 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***]**

no maximum routes

Параметры

vlan *VLAN-ID*	(Опционально) Укажите интерфейс VLAN, который необходимо отобразить. Если VLAN не указаны, будет отображена информация о группе IGMP Snooping для всех VLAN с включенной функцией IGMP Snooping.
IP-ADDRESS	(Опционально) Укажите IP-адрес группы, которую необходимо отобразить. Если IP-адрес не указан, будет отображена информация обо всех группах IGMP.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию о группе IGMP Snooping.

Пример

В данном примере показано, как отобразить информацию о группе IGMP Snooping.

```
Switch# show ip igmp snooping groups

IGMP Snooping Connected Group Membership:

VLAN ID  Group address    Source address   Exp(sec)  Interface
-------  ---------------  ---------------  --------  ---------
1        239.255.255.250        *          382       2/0/7

Total Entries: 1

Switch#
```

23.14. 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) Укажите VLAN. Если VLAN не указана, будет отображена информация об IGMP Snooping на всех VLAN с включенной функцией IGMP Snooping.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

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#
```

23.15. 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

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию о статической группе IGMP Snooping.

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#
```

23.16. show ip igmp snooping statistics

Данная команда используется для отображения информации о статистике IGMP Snooping на коммутаторе.

show ip igmp snooping statistics vlan [*VLAN-ID***]**

Параметры

vlan *VLAN-ID*	Укажите VLAN ID, который необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

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 1, Query 0
IGMPv2 Rx: Report 0, Query 0, Leave 0
IGMPv3 Rx: Report 0, Query 0
IGMPv1 Tx: Report 0, Query 0
IGMPv2 Tx: Report 0, Query 0, Leave 0
IGMPv3 Tx: Report 0, Query 0

Total Entries: 1

Switch#
```

24. Команды управления интерфейсом

24.1. clear counters

Данная команда используется для сброса всех счетчиков для интерфейса физического порта.

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

Параметры

all	Укажите, если необходимо сбросить счетчики для всех интерфейсов.
INTERFACE-ID	Укажите interface ID, если необходимо сбросить счетчик.
,	(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 сбросить счетчики для интерфейса физического порта.

Пример

В данном примере показан процесс сброса счетчиков для Ethernet 1/0/1.

```
Switch# clear counters interface eth 1/0/1
Switch#
```

24.2. description

Данная команда используется для добавления описания для интерфейса. Для удаления описания воспользуйтесь формой **no.**

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

Указанное описание соответствует объекту MIB «ifAlias», определенному в RFC 2233.

Пример

В данном примере показано, как добавить описание «Physical Port 10» на интерфейс Ethernet 1/0/10.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/10
Switch(config-if)# description "Physical Port 10"
Switch(config-if)#
```

24.3. interface

Данная команда используется для входа в режим Interface Configuration Mode для одного интерфейса. Для удаления интерфейса воспользуйтесь формой **no**.

interface *INTERFACE-ID*

no interface *INTERFACE-ID*

Параметры

INTERFACE-ID	Укажите идентификатор интерфейса (Interface ID). ID интерфейса состоит из типа интерфейса и номера интерфейса. Типы интерфейсов следующие: • ethernet – физический Ethernet – порт коммутатора любой среды. • vlan – интерфейс VLAN. • port-channel – агрегированный интерфейс port-

	channel • range – войдите в режим Interface Range Configuration Mode для нескольких интерфейсов. • combo copper ethernet – комбинированный медный Ethernet – порт коммутатора (combo copper media). • combo fiber ethernet – комбинированный оптический Ethernet – порт коммутатора (combo fiber media).

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для входа в режим Interface Configuration Mode для определенного интерфейса. Формат номера интерфейса зависит от типа интерфейса. Для интерфейсов физических портов пользователь не может войти в интерфейс если порт коммутатора не существует. Интерфейс физического порта не может быть удален командой **no**.

Используйте команду **interface Vlan** для создания интерфейса 3 уровня. Используйте команду **vlan** в режиме Global Configuration Mode, чтобы создать VLAN перед созданием интерфейса 3 уровня. Используйте команду **no interface Vlan**, чтобы удалить интерфейс 3 уровня.

Интерфейс port-channel автоматически создается, когда команда **channel-group** настроена для интерфейса физического порта. Интерфейс port-channel будет удален автоматически, если для команды **channel-group** не будет настроен интерфейс физического порта. Используйте команду **no interface Port-channel**, чтобы удалить port-channel.

Для интефейса null поддерживается интерфейс **null0**, и он не может быть удален.

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-channel 3
Switch(config-if)#

This example shows how to enter combo rj45 port interface configuration mode for
the interface ethernet 1/0/11
Switch# configure terminal
Switch(config)# interface combo copper ethernet 1/0/11
Switch(config-if-combo)#
```

24.4. interface range

Данная команда используется для входа в режим Interface Range Configuration Mode для нескольких интерфейсов.

interface [combo {copper | fiber }] range *INTERFACE-ID* **[, | -]**

Параметры

INTERFACE-ID	Укажите интерфейс физического порта.
,	(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

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 Interface Configuration Mode для диапазона портов от 1/0/1 до 1/0/5, и для порта 1/0/7.

```
Switch# configure terminal
Switch(config)# interface range ethernet 1/0/2-5,1/0/7
Switch(config-if-range)#

This example shows how to enter combo sfp port interface configuration mode for the range of ports 1/0/11 to 1/0/12
Switch# configure terminal
Switch(config)# interface combo fiber range ethernet 1/0/11-12
Switch(config-if-combo-range)#
```

24.5. show counters

Данная команда используется для отображения счетчиков для интерфейса физического порта.

show counters [interface *INTERFACE-ID***]**

Параметры

INTERFACE-ID	Указывает, что интерфейсом будет физический порт. Если интерфейс не указан, будут отображаться счетчики для всех интерфейсов.

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 статистики счетчиков для интерфейса.

Пример

В данном примере показано, как включить отображение счетчиков для Ethernet 1/0/1.

```
Switch#show counter interface eth 1/0/1

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
rxMulticastDropPkts              : 0
rxMTUDropPkts                    : 0

ifInErrors                       : 0
ifOutErrors                      : 0
ifInDiscards                     : 1175
ifInUnknownProtos                : 0
ifOutDiscards                    : 0
txDelayExceededDiscards          : 0

dot3StatsAlignmentErrors         : 0
dot3StatsFCSErrors               : 0
dot3StatsSingleColFrames         : 0
```

```
dot3StatsMultiColFrames            : 0
dot3StatsSQETestErrors             : 0
dot3StatsDeferredTransmisions      : 0
dot3StatsLateCollisions            : 0
dot3StatsExcessiveCollisions       : 0
dot3StatsInternalMacTransmitErrors : 0
dot3StatsCarrierSenseErrors        : 0
dot3StatsInternalMacReceiveErrors  : 0

linkChange                         : 1

Switch#
```

24.6. show interfaces

Данная команда используется для просмотра информации об интерфейсе.

show interfaces [*INTERFACE-ID* **[- | ,]]**

Параметры

INTERFACE-ID	(Опционально) Укажите физический порт, VLAN или другой интерфейс.
,	(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

Любой режим конфигурирования

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 для Ethernet 1/0/1.

```
Switch#show interfaces ethernet 1/0/1

Ethernet 1/0/1 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 excessive deferral: 0
  TX single collision: 0, TX excessive collision: 0
  TX late collision: 0

Switch#
```

24.7. 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. Если интерфейс не указан, отображаться будут счетчики для всех 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.
errors	(Опционально) Укажите для отображения счетчика ошибок.

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 статистики счетчиков порта коммутатора.

Пример

В данном примере показано, как отобразить счетчики на портах коммутатора 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 данном примере показано, как отобразить счетчики ошибок на портах коммутатора.

```
Switch#
Switch# show interfaces etherneter 1/0/1-8 counters errors

Port         Align-Err    Fcs-Err      UnderSize    OutDiscard   Carri-Sen
---------    --------     ---------    ----------   ----------   -------
ethernet 1/0/1     0            0            0            0            0
ethernet 1/0/2     0            0            0            0            0
ethernet 1/0/3     0            0            0            0            0
ethernet 1/0/4     0            0            0            0            0
ethernet 1/0/5     0            0            0            0            0
ethernet 1/0/6     0            0            0            0            0
ethernet 1/0/7     0            0            0            0            0
ethernet 1/0/8     0            0            0            0            0

Port         Single-Col   Multi-Col    Late-Col     Excess-Col   SQETest-Err
---------    --------     ---------    ----------   ----------   ------
ethernet 1/0/1     0            0            0            0            0
ethernet 1/0/2     0            0            0            0            0
ethernet 1/0/3     0            0            0            0            0
ethernet 1/0/4     0            0            0            0            0
ethernet 1/0/5     0            0            0            0            0
ethernet 1/0/6     0            0            0            0            0
ethernet 1/0/7     0            0            0            0            0
ethernet 1/0/8     0            0            0            0            0

Port         DeferredTx   IntMacTx     IntMacRx
---------    ----------   --------     ----------
ethernet 1/0/1     0            0            0
ethernet 1/0/2     0            0            0
ethernet 1/0/3     0            0            0
ethernet 1/0/4     0            0            0
ethernet 1/0/5     0            0            0
ethernet 1/0/6     0            0            0
ethernet 1/0/7     0            0            0
ethernet 1/0/8     0            0            0

total entries: 8
Switch#
```

24.8. 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) 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

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для просмотра состояния подключения портов коммутатора.

Пример

В данном примере показано, как включить отображение состояния подключения портов коммутатора.

```
Switch# show interfaces etherneter 1/0/1-8 status

Port         Status          MAC Address         VLAN   Duplex      Speed
Type
-----------  --------------  ------------------  -----  ----------  -----------
---------
ethernet 1/0/1     Not-Connected   00-00-04-01-02-02   1      Auto        Auto
10GBASE-T
ethernet 1/0/2     Not-Connected   00-00-04-01-02-03   1      Auto        Auto
10GBASE-T
ethernet 1/0/3     Not-Connected   00-00-04-01-02-04   1      Auto        Auto
10GBASE-T
ethernet 1/0/4     Not-Connected   00-00-04-01-02-05   1      Auto        Auto
10GBASE-T
ethernet 1/0/5     Connected       00-00-04-01-02-06   1      Auto-Full   Auto-
1000M
10GBASE-T
ethernet 1/0/6     Not-Connected   00-00-04-01-02-07   1      Auto        Auto
10GBASE-T
ethernet 1/0/7     Not-Connected   00-00-04-01-02-08   1      Auto        Auto
10GBASE-T
ethernet 1/0/8     Not-Connected   00-00-04-01-02-09   1      Auto        Auto
10GBASE-T
```

24.9. shutdown

Данная команда используется для отключения интерфейса. Для включения интерфейса воспользуйтесь формой **no**.

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. 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 ethernet 1/0/1
Switch(config-if)# shutdown
```

25. Команды IP Utility

25.1. traceroute

Данная команда используется для отображения пути передачи от узла к узлу через сеть IP от коммутатора к указанному узлу назначения (destination).

traceroute {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [probe** *NUMBER***] [timeout** *SECONDS***] [max-ttl** *TTL***] [port** *DEST-PORT***]**

Параметры

IP-ADDRESS	Укажите IPv4-адрес узла назначения.
IPV6-ADDRESS	Укажите IPv6-адрес системы, который необходимо обнаружить.
probe	(Опционально) Укажите количество датаграмм, которое необходимо отослать.
timeout *SECONDS*	(Опционально) Укажите время ожидания ответа в секундах.
max-ttl *TTL*	(Опционально) Укажите максимальное значение TTL для исходящих UDP-датаграмм.
port *DEST-PORT*	(Опционально) Укажите количество базовых UDP-портов назначения, используемых в исходящих датаграммах.

По умолчанию

По умолчанию отправляются три 64-байтовые UDP-датаграммы с начальным значением TTL, равным 1.

Максимальное значение TTL – 30.

Тайм-аут – 5 секунд.

Номер UDP-порта назначения – 33434.

Режим ввода команды

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-датаграммы на узел назначения с полем TTL 1. Если

маршрутизатор обнаруживает значение TTL 1 или 0, датаграмма 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 датаграмму на следующий маршрутизатор. Обнаружив TTL со значением 1, второй маршрутизатор отбрасывает датаграмму и отправляет на источник сообщение time exceeded. Этот процесс продолжается до тех пор, пока значение TTL не увеличится настолько, чтобы датаграмма могла достичь узла назначения (или до тех пор, пока не будет достигнуто максимальное значение TTL).

Чтобы определить, достигла ли датаграмма своего назначения, **traceroute** устанавливает очень большое значение для UDP-порта назначения в датаграмме, так что оно вряд ли будет использоваться узлом назначения. Если узел получает датаграмму с нераспознанным номером порта, на источник будет отправлена ошибка ICMP Port Unreachable. Данное сообщение свидетельствует **traceroute** о том, что датаграмма достигла назначения.

Пример

В данном примере показано, как выполнить трассировку маршрута к узлу с IP-адресом назначения (destination) 8.8.8.8.

```
Switch# traceroute 8.8.8.8 probe 8
 1    ms        192.168.0.1
 2    ms        168.95.23.118
 2    ms        220.128.9.242
 2    ms        220.128.9.13
 3    ms        142.250.169.122
 4    ms        108.170.244.129
 2    ms        8.8.8.8

Trace Complete
```

25.2. ping

Данная команда используется для диагностики базового сетевого соединения.

ping {*IP-ADDRESS* **|** *IPV6-ADDRESS* **[***VLAN-ID***]} [count** *TIMES***] [timeout** *SECONDS***] [source {***IP-ADDRESS* **|** *IPV6-ADDRESS***}]**

Параметры

IP-ADDRESS	Укажите IPv4-адрес узла назначения (destination).
IPV6-ADDRESS	Укажите IPv6-адрес системы, который необходимо обнаружить.
VLAN-ID	(Опционально) IP-адрес VLAN ID для получения индекса интерфейса.
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***}**	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

Если параметр **timeout** не указан, значение тайм-аута будет равно 1 секунде.

Режим ввода команды

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 данном примере показано, как протестировать узел с IP-адресом 211.21.180.1 с параметром count, равным 4.

```
Switch#ping 211.21.180.1 count 4

Reply from 211.21.180.1, time=10ms
Reply from 211.21.180.1, time<10ms
Reply from 211.21.180.1, time<10ms
Reply from 211.21.180.1, time<10ms

 Ping Statistics for 211.21.180.1
 Packets: Sent =4, Received =4, Lost =0


Switch#
```

В данном примере показано, как 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#
```

26. Команды Jumbo Frame

26.1. max-rcv-frame-size

Данная команда используется для настройки максимально допустимого размера Ethernet-фреймов. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

max-rcv-frame-size *BYTES*

no max-rcv-frame-size

Параметры

BYTES	Укажите максимально допустимый размер Ethernet-фреймов.

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 4/0/1. Указанное значение – 6000 байт.

```
Switch# configure terminal
Switch(config)#interface ethernet 4/0/1
Switch(config-if)# max-rcv-frame-size 6000
Switch(config-if)#
```

27. Команды Link Aggregation Control Protocol (LACP)

27.1. channel-group

Данная команда используется для привязки интерфейса к агрегированной группе (channel group). Для удаления интерфейса из агрегированной группы воспользуйтесь формой **no**.

channel-group *CHANNEL-NO* **mode {on | active | passive}**

no channel-group

Параметры

CHANNEL-NO	Укажите channel group ID. Доступный диапазон значений: от 1 до 8.
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.

Для удаления интерфейса из channel group воспользуйтесь формой **no**. Если после удаления порта в channel group не осталось портов-участников, channel group будет удалена автоматически. Port-channel также может быть удален командой **no interface port-channel**.

Если на порту включена функция Security, данный порт нельзя указать в качестве участника channel group.

Пример

В данном примере показано, как привязать интерфейсы от Ethernet 1/0/4 по 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 1/0/4-5
Switch(config-if)# channel-group 3 mode active
Switch(config-if)#
```

27.2. lacp port-priority

Данная команда используется для настройки приоритета порта. Для возврата приоритета порта к настройкам по умолчанию воспользуйтесь формой **no**.

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 1/0/4-5
Switch(config-if)# lacp port-priority 20000
Switch(config-if)#
```

27.3. lacp timeout

Данная команда используется для настройки таймера LACP Long или LACP Short. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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. Как только партнер распознает эту информацию в полученном PDU, регулярные передачи LACP PDU будут отправляться с интервалом в 1 секунду.
long	Укажите, чтобы выбрать значение 90 секунд для интервала, по истечении которого полученная информация о LACPDU будет объявлена недействительной. Как только партнер распознает эту информацию в полученном PDU, регулярные передачи LACP PDU будут отправляться с интервалом в 30 секунд.

По умолчанию

Режим LACP Timeout по умолчанию – **long**.

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)#
```

27.4. lacp system-priority

Данная команда используется для настройки приоритета системы. Для возврата приоритета системы к настройкам по умолчанию воспользуйтесь формой **no**.

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. Когда максимальное количество фактических участников превышает ограничение, при помощи приоритета порта коммутатор определяет, в каком режиме функционирует порт – Backup Mode или Active Mode. Приоритет системы LACP определяет коммутатор, контролирующий приоритет порта. Приоритеты портов других коммутаторов будут игнорированы.

Чем ниже значение, тем выше приоритет. Если у двух коммутаторов совпадает приоритет системы, приоритет будет определяться при помощи ID/MAC системы LACP. Команда приоритета системы LACP применима для всех LACP port-channel коммутатора.

Пример

В данном примере показано, как сконфигурировать приоритет системы LACP. Указанное значение – 30000.

```
Switch# configure terminal
Switch(config)#lacp system-priority 30000
Switch(config)#
```

27.5. port-channel load-balance

Данная команда используется для настройки алгоритма Load Balancing (балансировка нагрузки), используемого коммутатором для распределения пакетов на порты одного канала. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

port-channel load-balance { dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac | l4-dst-port | l4-src-port | l4-src-dst-port }

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.
l4-dst-port	Укажите, чтобы коммутатор проверил порт назначения.
l4-src-port	Укажите, чтобы коммутатор проверил порт источника.
l4-src-dst-port	Укажите, чтобы коммутатор проверил порт источника и порт назначения.

По умолчанию

Алгоритм Load Balancing по умолчанию – **src-mac**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы указать Load Balancing. Можно указать только один алгоритм.

Пример

В данном примере показано, как сконфигурировать Load Balancing **src-ip**.

```
Switch# configure terminal
Switch(config)#port-channel load-balance src-ip
Switch(config)#
```

27.6. 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

Любой режим конфигурирования

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 3
  Member Ports: 2, Maxports = 12, Protocol: LACP
  Description:
                        LACP          Port        Port
  Port          Flags   State         Priority    Number
  ------------------------------------------------------
  eth1/0/4      FA      down          20000       0
  eth1/0/5      FA      down          20000       0

Switch#
```

28. Команды Link Layer Discovery Protocol (LLDP)

28.1. clear lldp counters

Данная команда используется для удаления статистики LLDP.

clear lldp counters [all | interface *INTERFACE-ID* **[, | -]]**

Параметры

all	Укажите, чтобы обнулить счетчик LLDP для всех интерфейсов и статистики Global LLDP.
interface *INTERFACE-ID*	Укажите интерфейс, на котором необходимо обнулить счетчик LLDP.
,	(Опционально) Используется для перечисления нескольких физических интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона физических 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 выбраны дополнительные параметры, будут обнулены только счетчики Global LLDP.

Пример

В данном примере показано, как удалить статистику LLDP.

```
Switch# clear lldp counters all
Switch#
```

В данном примере показано, как удалить статистику LLDP на интерфейсе ethernet 1/0/1.

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

28.2. 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.
,	(Опционально) Используется для перечисления нескольких физических интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона физических 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#
```

В данном примере показано, как удалить информацию, полученную от соседних устройств, на интерфейсе ethernet 1/0/1.

```
Switch# clear lldp table interface ethernet 1/0/1
Switch#
```

28.3. lldp dot1-tlv-select

Данная команда используется для указания дополнительных настроек TLV (type-length-value) в указанном в пределах IEEE 802.1 наборе TLV, которые будут переданы и инкапсулированы в LLDPDU, а затем отправлены на соседние устройства. Для отключения передачи TLV воспользуйтесь формой **no**.

lldp dot1-tlv-select {port-vlan | vlan-name [*VLAN-ID* **[, | -]] | protocol-identity [***PROTOCOL-NAME***]}**

no lldp dot1-tlv-select {port-vlan | vlan-name [*VLAN-ID* **[, | -]] | protocol-identity [***PROTOCOL-NAME***]}**

Параметры

port-vlan	Укажите Port VLAN ID TLV, который необходимо отправить. Port VLAN ID TLV – это дополнительный TLV фиксированной длины, который позволяет порту VLAN Bridge анонсировать PVID (Port VLAN Identifier), который будет ассоциирован с нетегированными или тегированными по приоритету кадрами.
vlan-name	Укажите VLAN Name TLV, который необходимо отправить. VLAN Name TLV – это дополнительный TLV, который позволяет IEEE 802 LAN station, совместимой с IEEE 802.1Q, анонсировать присвоенное имя любой VLAN, с которой она сконфигурирована.
VLAN-ID **[, | -]**	(Опционально) Укажите VLAN ID в VLAN Name TLV. Доступный диапазон значений: от 1 до 4094. Разделите непоследовательный VLAN ID запятой. Используйте дефис для обозначения диапазона VLAN ID. Если VLAN ID не указан все применимые VLAN будут отправлены. При использовании данной команды в форме **no**, если не указан VLAN ID, все сконфигурированные VLAN для VLAN Name TLV будут удалены и VLAN Name TLV отправлен не будет.
protocol-identity [*PROTOCOL-NAME***]**	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. Допустимые для PROTOCOL-NAME строки: **eapol**: Extensible Authentication Protocol (EAP) по LAN **lacp**: Link Aggregation Control Protocol

	gvrp: GARP VLAN Registration Protocol **stp**: Spanning Tree Protocol Имя протокола является необязательным. Если конкретная строка протокола не указана, все протоколы выбираются или отменяются в форме **no**.

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 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-identity lacp
Switch(config-if)#
```

28.4. lldp dot3-tlv-select

Данная команда используется для указания дополнительных настроек TLV в указанном в пределах IEEE 802.3 наборе TLV, которые будут инкапсулированы в LLDPDU, а затем отправлены на соседние устройства. Для отключения передачи TLV воспользуйтесь формой **no**.

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	(Опционально) Укажите Power Via MDI TLV, который необходимо отправить. Три варианта IEEE 802.3 PMD (10BASE-T, 100BASE-TX и 1000BASE-T) обеспечивают подачу питания подключенным системам без питания. Power Via MDI TLV позволяет сетевому управлению анонсировать и обнаруживать возможности поддержки питания MDI отправляющей сети IEEE 802.3 LAN.
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.

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)#
```

28.5. lldp fast-count

Данная команда используется для настройки количества отправлемых пакетов Fast Start (LLDP MED Fast Start Repeat Count Option)на коммутаторе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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 данном примере показано, как сконфигурировать количество отправляемых пакетов Fast Start.

```
Switch# configure terminal
Switch(config)#lldp fast-count 10
Switch(config)#
```

28.6. lldp hold-multiplier

Данная команда используется для настройки множителя удержания для обновлений LLDP на коммутаторе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

lldp hold-multiplier *VALUE*

no hold-multiplier

Параметры

VALUE	Укажите множитель 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 является множителем 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)#
```

28.7. lldp management-address

Данная команда используется для настройки адреса управления (Management Address), который будет анонсирован на физическом интерфейсе. Для удаления настроек воспользуйтесь формой **no**.

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 является одним из адресов системных интерфейсов, то адрес не будет отправлен.

Если при использовании команды **lldp management-address** не указан ни один адрес, коммутатор обнаружит по крайней мере один IPv4/IPv6-адрес в VLAN с самым низким VLAN ID. Если подходящих IPv4/IPv6-адресов нет, Management Address TLV анонсирован не будет. После того, как администратор сконфигурировал адрес, оба адреса управления по умолчанию (IPv4 и IPv6) станут неактивны и не будут отправлены. IPv4/IPv6-адрес по умолчанию снова станет активен, если все сконфигурированные адреса будут удалены. Используйте данную команду несколько раз, чтобы создать несколько адресов управления IPv4/IPv6.

Используйте команду **no lldp management-address** без адреса управления, чтобы отключить адрес управления, анонсированный в LLDPDU. При отсутствии в списке действительного адреса управления, Management Address TLV отправлен не будет.

Пример

В данном примере показано, как настроить адрес управления IPv4 на интерфейсах Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch# configure terminal
Switch(config)#interface range ethernet 1/0/1-1/0/2
Switch(config-if-range)# lldp management-address 10.1.1.1
Switch(config-if-range)#
```

В данном примере показано, как настроить адрес управления IPv6 на интерфейсах Ethernet 1/0/3 и Ethernet 1/0/4.

```
Switch# configure terminal
Switch(config)#interface range ethernet 1/0/3-1/0/4
Switch(config-if-range)# lldp management-address FE80::250:A2FF:FEBF:A056
Switch(config-if-range)#
```

В данном примере показано, как удалить адрес управления 10.1.1.1 из интерфейсов Ethernet 1/0/1 и Ethernet 1/0/2. Если 10.1.1.1 является последним, то Management Address TLV отправлен не будет.

```
Switch# configure terminal
Switch(config)#interface range ethernet 1/0/1-1/0/2
Switch(config-if-range)# no lldp management-address 10.1.1.1
Switch(config-if-range)#
```

В данном примере показано, как удалить адрес управления FE80::250:A2FF:FEBF:A056 из интерфейсов Ethernet 1/0/3 и Ethernet 1/0/4.

```
Switch# configure terminal
Switch(config)#interface range ethernet 1/0/3-1/0/4
Switch(config-if-range)# no lldp management-address FE80::250:A2FF:FEBF:A056
Switch(config-if-range)#
```

В данном примере показано, как удалить все адреса управления из интерфейса Ethernet 1/0/5. В этом случае на Ethernet 1/0/5 Management Address TLV отправлен не будет.

```
Switch# configure terminal
Switch(config)#interface ethernet 1/0/5
Switch(config-if)# no lldp management-address
Switch(config-if)#
```

28.8. lldp med-tlv-select

Данная команда используется для указания дополнительного LLDP-MED TLV, который будет передан, инкапсулирован в LLDPDU и отправлен на соседние устройства. Для отключения передачи TLV воспользуйтесь формой **no**.

lldp med-tlv-select [capabilities | inventory-management]

no lldp med-tlv-select [capabilities | inventory-management]

Параметры

capabilities	(Опционально) Укажите, чтобы передать LLDP-MED Capabilities TLV.
inventory-management	(Опционально) Укажите, чтобы передать LLDP-MED

Inventory Management TLV.

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)#
```

28.9. lldp receive

Данная команда используется для того, чтобы включить на физическом интерфейсе получение LLDP-сообщений. Для отключения получения LLDP-сообщений воспользуйтесь формой **no**.

lldp receive

no lldp receive

Параметры

Нет.

По умолчанию

По умолчанию функция LLDP выключена 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 сообщений LLDP.

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

28.10. lldp reinit

Данная команда используется для настройки минимального интервала перед повторной инициализацией на коммутаторе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

lldp reinit *SECONDS*

no lldp reinit

Параметры

SECONDS	Укажите время задержки инициализации LLDP на интерфейсе. Доступный диапазон значений: от 1 до 10 секунд.

По умолчанию

Значение по умолчанию – 2 секунды.

Режим ввода команды

Global Configuration Mode

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)#
```

28.11. lldp run

Данная команда используется для глобального включения LLDP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

28.12. lldp forward

Данная команда используется для включения состояния LLDP Forwarding. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

28.13. lldp tlv-select

Данная команда используется для выбора Type-Length-Value (TLV) в наборе 802.1AB Basic Management, а также для передачи TLV и его инкапсулирования в LLDPDU с последующей отправкой на соседние устройства. Для отключения данной опции воспользуйтесь формой **no**.

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 сетевому управлению анонсировать описание порта IEEE 802 LAN.
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 TLV 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 TLV 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)#
```

28.14. lldp transmit

Данная команда используется для включения анонсирования/передачи LLDP. Для отключения передачи LLDP воспользуйтесь формой **no**.

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)#
```

28.15. lldp tx-delay

Данная команда используется для настройки таймера Transmission Delay, определяющего минимальный интервал между отправкой LLDP-сообщений на основе постоянно изменяющегося содержания MIB. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

28.16. lldp tx-interval

Данная команда используется для настройки интервала LLDPDU Transmission на коммутаторе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

28.17. snmp-server enable traps lldp

Данная команда используется для включения отправки LLDP Trap и LLDP-MED Trap.

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 **snmp-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)#
```

28.18. 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)#
```

28.19. 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

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить общие настройки функции LLDP.

Пример

В данном примере показано, как отобразить общие настройки функции LLDP.

```
Switch#show lldp

LLDP System Information
    Chassis ID Subtype        : MAC Address
    Chassis ID                : 3C-1E-04-A1-CC-00
    System Name               : Switch
    System Description        : Gigabit Ethernet SmartPro 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         : 1.00.012
    Software Revision         : 1.30.003
    Serial Number             :
    Manufacturer Name         : D-Link Corporation
    Model Name                : DXS-1210-28XMP Gigabit Ethernet
    Asset ID                  :
    PoE Device Type           : PSE Device
    PoE PSE Power Source      : Primary

LLDP Configurations
    LLDP State                : Disabled
    LLDP Forward State        : Disabled
    Message TX Interval       : 30
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

28.20. 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, чтобы отобразить конфигурацию LLDP для определенного интерфейса. Доступны только физические интерфейсы.
,	(Опционально) Используется для перечисления нескольких физических интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона физических интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

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: ethernet 1/0/1
------------------------------------------------------------------------------
Port ID                                                 :ethernet 1/0/1
Admin Status                                            :TX and RX
Notification                                            :Disabled
Basic Management TLVs:
    Port Description                                    :Enabled
    System Name                                         :Enabled
    System Description                                  :Enabled
    System Capabilities                                 :Enabled
    Enabled Management Address:
        (None)
IEEE 802.1 Organizationally Specific TLVs:

    Port VLAN ID                                        :Enabled
    Enabled Port_and_Protocol_VLAN_ID
        1, 2, 3
    Enabled VLAN Name
        1-3
    Enabled Protocol_Identity
        EAPOL, LACP, GVRP, STP
IEEE 802.3 Organizationally Specific TLVs:

    MAC/PHY Configuration/Status                        :Enabled
    Link Aggregation                                    :Disabled
    Maximum Frame Size                                  :Disabled

LLDP-MED Organizationally Specific TLVs:

    LLDP-MED Capabilities TLV                           :Enabled
    LLDP-MED Network Policy TLV                         :Disabled
    LLDP-MED Extended Power Via MDI PSE TLV             :Disabled
    LLDP-MED Inventory TLV                              :Disabled


Switch#
```

Отображаемые параметры

Enabled Management Address	Отображает включенные IPv4/IPv6-адреса. «(None)» означает, что пользователь не сконфигурировал адрес управления (Management Address) при помощи команды **lldp management-address** или включенные IPv4/IPv6-адреса по умолчанию не применяются.
Enabled Port and Protocol VLAN ID	Отображает включенные Port and Protocol VLAN. В список VLAN включены сконфигурированные и включенные VLAN. При отсутствии сконфигурированных PPVID VLAN отображается «(None)».

Enabled VLAN Name	Отображает включенные VLAN для отправки VLAN Name TLV. В список VLAN включены сконфигурированные и включенные VLAN. При отсутствии сконфигурированных VLAN для VLAN Name TLV отображается «(None)».
Enabled Protocol Identity	Отображает включенную строку протокола для Protocol Identity TLV. При отсутствии включенных протоколов для Protocol Identity TLV отображается «(None)».

28.21. 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 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

Любой режим конфигурирования

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: ethernet 1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : ethernet 1/0/1
Port Description                         : D-Link Corporation DXS-1210-28XMP
                                           1.30.003 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
    (None)
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: ethernet 1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : ethernet 1/0/1
Port Description                         : D-Link Corporation DXS-1210-28XMP
                                           1.30.003 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: ethernet 1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : ethernet 1/0/1
Port Description                         : D-Link Corporation DXS-1210-28XMP
                                           1.30.003 Port 1 on Unit 1


Switch#
```

28.22. 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-ADDRES	(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

Любой режим конфигурирования

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                              : 1.3.6.1.4.1.171.10.118.2
    Advertising Ports                : -

Address 2 :
-----------------------------------------------
    Subtype                          : IPv4
    Address                          : 10.90.90.90
    IF Type                          : IfIndex
    OID                              : 1.3.6.1.4.1.171.10.118.2
    Advertising Ports                : -

Total Entries : 2

Switch#
```

28.23. 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.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
brief	(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

Любой режим конфигурирования

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 neighbor interface ethernet 1/0/9 detail

Port ID : ethernet 1/0/9
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                          : MAC Address
    Chassis ID                                  : 00-01-02-03-04-05
    Port ID Subtype                             : Local
    Port ID                                     : ethernet 1/0/5
    Port Description                            : RMON Port
    System Name                                 : Switch1
    System Description                          : Stackable Ethernet Switch
    System Capabilities Supported               : Repeater, Bridge
    System Capabilities Enabled                 : Repeater, Bridge
    Management Address Count                    : 0
        (None)
    Port VLAN ID                                : 0
    PPVID Entries Count                         : 0
        (None)
    VLAN Name Entries Count                     : 0
        (None)
    Protocol ID Entries Count                   : 0
        (None)
    MAC/PHY Configuration/Status                : (None)
    Power Via MDI                               : (None)
    Link Aggregation                            : (None)
    Maximum Frame Size                          : 0
    Unknown TLVs Count                          : 0
        (None)
LLDP-MED capabilities                       :
LLDP-MED device class                    : Endpoint device class III
    LLDP-MED capabilities support           :
          LLDP-MED capabilities                 : Support
          Network Policy                        : Support
          Location identification               : Not Support
          Extended power via MDI                : Support
          Inventory                             : Support
       LLDP-MED capabilities enabled              :
          LLDP-MED capabilities                 : Enabled
          Network Policy                        : Enabled
          Location identification               : Enabled
          Extended power via MDI                : Enabled
          Inventory                             : Enabled
   Extended power via MDI                       :
             Power device type                  : PD device
             Power Source                       : from PSE
             Power request                      : 8 watts
Network policy                              :
        Application type                        : Voice
        VLAN ID                                 : -
        Priority                                : -
        DSCP                                    : -
        Unknown                                 : True
        Tagged                                  : -
```

```
    Inventory Management                        :
        (None)

Switch#
```

В данном примере показано, как отобразить информацию о Remote LLDP в стандартном формате.

```
Switch# show lldp neighbor interface ethernet 1/0/1

Port ID : 1
------------------------------------------------------------------------
Remote Entities Count : 2
Entity 1
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-01
      Port ID Subtype               : Local
      Port ID                       : ethernet 3/0/1
      Port Description              : RMON Port 3 on Unit 1
      System Name                   : Switch1
      System Description            : Stackable Ethernet Switch
      System Capabilities Supported : Repeater, Bridge
      System Capabilities Enabled : Repeater, Bridge
      Management Address Count      : 1
      Port VLAN ID                  : 1
      PPVID Entries Count           : 5
      VLAN Name Entries Count       : 3
      Protocol ID Entries Count     : 2
      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)
    Inventory Management            : (See Detail)
    Unknown TLVs Count              : 2
Entity 2
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-02
      Port ID Subtype               : Local
      Port ID                       : ethernet 2/0/1
      Port Description              : RMON Port 1 on Unit 2
      System Name                   : Switch2
      System Description            : Stackable Ethernet Switch
System Capabilities Supported : Repeater, Bridge
System Capabilities Enabled   : Repeater, Bridge
      Management Address Count      : 2
      Port VLAN ID                  : 1
      PPVID Entries Count           : 5
      VLAN Name Entries Count       : 3
      Protocol Id Entries Count     : 2
      MAC/PHY Configuration Status  : (See Detail)
      Power Via MDI                 : (See Detail)
      Link Aggregation              : (See Detail)
      Maximum Frame Size            : 1536
      LLDP-MED capabilities         : (See Detail)
      Extended power via MDI        : (See Detail)
```

```
Network policy                      : (See Detail)
    Inventory Management            : (See Detail)
Unknown TLVs Count            : 2

Switch#
```

В данном примере показано, как отобразить информацию о соседних устройствах на интерфейсах от Ethernet 1/0/1 до Ethernet 1/0/2 в кратком формате.

```
Switch# show lldp neighbor interface ethernet 1/0/1-1/0/2 brief

Port ID: ethernet 1/0/1
------------------------------------------------------------
Remote Entities Count : 2
Entity 1
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-01
      Port ID Subtype               : Local
      Port ID                       : ethernet 3/0/1
      Port Description              : RMON Port 1 on Unit 3
Entity 2
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-02
      Port ID Subtype               : Local
      Port ID                       : ethernet 4/0/1
      Port Description              : RMON Port 1 on Unit 4

Port ID : ethernet 1/0/2
------------------------------------------------------------------------
Remote Entities Count : 3
Entity 1
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-03
      Port ID Subtype               : Local
      Port ID                       : ethernet 2/0/1
      Port Description              : RMON Port 2 on Unit 1
Entity 2
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-04
      Port ID Subtype               : Local
      Port ID                       : ethernet 2/0/2
      Port Description              : RMON Port 2 on Unit 2
Entity 3
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-05
      Port ID Subtype               : Local
      Port ID                       : ethernet 3/0/2
      Port Description              : RMON Port 2 on Unit 3

Total Entries: 2

Switch#
```

28.24. 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

Любой режим конфигурирования

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   : 7958183
Total Inserts      : 7
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.

28.25. 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.
,	(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

Любой режим конфигурирования

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 4.

```
Switch# show lldp traffic interface ethernet 1/0/4

Port ID : eth1/0/4
----------------------------------------
Total Transmits                     : 171
Total Discards                      : 7
Total Errors                        : 7
Total Receives                      : 7
Total TLV Discards                  : 0
Total TLV Unknows                   : 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.

28.26. show snmp-server traps lldp

Данная команда используется для отображения информации о состоянии LLDP snmp-server traps.

show snmp-server traps lldp

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить глобальную информацию о LLDP traps на коммутаторе.

Пример

В данном примере показано, как отобразить глобальную информацию о LLDP traps.

```
Switch#show snmp-server traps lldp

  lldp                          : Disabled
  lldp med                      : Disabled
Switch#
```

29. Команды Loopback Detection (LBD)

29.1. loopback-detection (Global)

Данная команда используется для включения функции Loopback Detection глобально. Для отключения функции глобально воспользуйтесь формой **no**.

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, если соседнее устройство не поддерживает функцию LBD.

Если включен режим port-based, порт, на котором включена функция LBD, будет отправлять нетегированные пакеты port-based LBD, чтобы обнаружить петлю. При наличии на пути петли передаваемый пакет вернется на тот же порт, или на другой порт того же устройства. При обнаружении портом, на котором включена функция LBD, петли, на порту будет отключена передача и получение пакетов.

Если включен режим VLAN-based, порт будет периодически отправлять пакеты VLAN-based LBD на каждую VLAN, членом которой является данный порт, и на которой включена функция LBD. Если порт является тегированным членом VLAN, будут отправлены тегированные пакеты LBD. Если порт является нетегированным членом VLAN, будут отправлены нетегированные пакеты LBD. При наличии на пути VLAN петли, передача и получение пакетов будет временно остановлена на том порту закольцованной VLAN, где была обнаружена петля.

Если порт, на котором отключена функция LBD, получает пакет LBD и обнаруживает, что

пакет отправлен системой, возможны два варианта: если тип данного пакета – port-based LBD, будет заблокирован порт отправления, а если тип пакета – VLAN-based LBD, будет заблокирована VLAN порта отправления.

Если на порту сконфигурирован режим VLAN-based, а порт является нетегированным членом нескольких VLAN, будет отправлен один нетегированный пакет LBD на каждую VLAN с указанием номера VLAN в поле VLAN пакета.

Восстановить порт, отключенный из-за ошибки, можно двумя способами: используйте команду **errdisable recovery cause loopback-detect**, чтобы включить автовосстановление, или восстановите порт вручную, применив сначала команду **shutdown**, а затем команду **no shutdown**.

Заблокированную VLAN можно восстановить автоматически, применив команду **errdisable recovery cause loopback-detect**. VLAN также можно восстановить вручную, применив сначала команду **shutdown**, а затем команду **no shutdown**.

Пример

В данном примере показано, как включить функцию LBD глобально и установить режим обнаружения port-based.

```
Switch# configure terminal
Switch(config)#loopback-detection
Switch(config)# loopback-detection mode port-based
Switch(config)#
```

29.2. loopback-detection (Interface)

Данная команда используется для включения функции LBD на интерфейсе. Для отключения данной функции на интерфейсе воспользуйтесь формой **no**.

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

Используйте данную команду, чтобы включить функцию LBD на интерфейсе. Команда применяется для конфигурирования физических портов и port-channel.

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)#
```

29.3. loopback-detection interval

Данная команда используется для конфигурирования временного интервала. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

loopback-detection interval *SECONDS*

no loopback-detection interval

Параметры

interval *SECONDS*	Укажите интервал передачи пакетов LBD. Доступный диапазон значений: от 1 до 32767.

По умолчанию

Интервал по умолчанию – 10 секунд.

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)#
```

29.4. loopback-detection vlan

Данная команда используется для того, чтобы включить функцию LBD на VLAN. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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 команды

Используйте данную команду, чтобы сконфигурировать список VLAN, на которых включена функция LBD. Настройки команды будут применены, если на порту сконфигурирован режим обнаружения петли VLAN-based.

Если список VLAN ID пуст, 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)#
```

29.5. show loopback-detection

Данная команда используется для отображения текущих настроек LBD.

show loopback-detection [interface *INTERFACE-ID* **[, | -] | port-channel** <*1-8*>**]**

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.
port-channel <*1-8*>	(Опционально) Укажите агрегированную группу (Channel Group), которую необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

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 : Enabled
Detection Mode : vlan-based
LBD enabled VLAN : all VLANs
Interval         : 20 seconds
Action           : Shut-down

Interface         Loopback Detection State  Result         Time Left(sec)
-------------     ------------------------  -------------- -------------
eth1/0/3               Disabled             Normal             0
eth1/0/4               Disabled             Normal             0
eth1/0/5               Disabled             Normal             0
eth1/0/6               Disabled             Normal             0
eth1/0/7               Disabled             Normal             0
eth1/0/8               Disabled             Normal             0
eth1/0/9               Disabled             Normal             0
eth1/0/10              Disabled             Normal             0
eth1/0/11              Enabled              Loop on VLAN 1     infinite
eth1/0/12              Enabled              Loop on VLAN 1     infinite
Port-Channel1          Disabled             Normal             0

Switch#
```

В данном примере показано, как отобразить статус функции LBD для интерфейса Ethernet 1/0/1.

```
Switch# show loopback-detection interface eth 1/0/1

Interface         Loopback Detection State  Result         Time Left(sec)
-------------     ------------------------  -------------- -------------
eth1/0/11              Enabled              Loop on VLAN 1     infinite

Switch#
```

В данном примере показано, как отобразить статус функции LBD для port-channel 2.

```
Switch# show loopback-detection interface port-channel 2

Interface         Loopback Detection State  Result         Time Left(sec)
-------------     ------------------------  -------------- -------------
Port-Channel1          Disabled             Normal             0

Switch#
```

Отображаемые параметры

Interface	Отображает порт, на котором включена функция LBD.
Result	Отображает, обнаружена ли петля.

Time Left	Отображает время, оставшееся до автовосстановления.

29.6. snmp-server enable traps loopback-detection

Данная команда используется для включения отправки SNMP-уведомлений для LBD. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

snmp-server enable traps loopback-detection

no snmp-server enable traps loopback-detectio

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 или отключить отправку SNMP-уведомлений для LBD.

Пример

В данном примере показано, как включить отправку SNMP-уведомлений для LBD.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps loopback-detection.
Switch(config)#
```

29.7. show snmp-server traps

Данная команда используется для отображения состояния SNMP-уведомлений для LBD. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

show snmp-server traps loopback-detection

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить состояние SNMP-trap для LBD.

Пример

В данном примере показано, как отобразить информацию о состоянии SNMP-уведомлений для LBD.

```
Switch# show snmp-server traps loopback-detection

Loopback Detection Trap State: disable

Switch#
```

29.8. loopback-detection action

Данная команда используется для настройки режима LBD. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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

Нет.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить режим LBD.

Пример

В данном примере показано, как настроить режим LBD.

```
Switch(config)# loopback-detection action shutdown
Switch(config)#
```

30. Команды Mirror

30.1. monitor session destination interface

Данная команда используется для настройки интерфейса назначения (destination) для сессии мониторинга, позволяя отслеживать пакеты на портах источника (source) через порт назначения. Для удаления сессии мониторинга или интерфейса назначения воспользуйтесь формой **no**.

monitor session *SESSION-NUMBER* **destination interface {***INTERFACE-ID* **| port-channel** *<1-8>***}**

no monitor session *SESSION-NUMBER*

Параметры

session *SESSION-NUMBER*	Укажите номер сессии мониторинга. Доступный диапазон значений: от 1 до 2.
interface *INTERFACE-ID*	Укажите интерфейс назначения для сессии мониторинга.
port-channel *<1-8>*	Укажите агрегированную группу (Channel Group) для сессии мониторинга.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить интерфейс назначения для локальной сессии мониторинга.

В качестве интерфейсов назначения для сессий мониторинга можно использовать физические порты и port-channel. Для сессии мониторинга можно указать несколько интерфейсов источника, но только один интерфейс назначения. Интерфейс не может быть одновременно интерфейсом источника одной сессии и портом назначения другой сессии. Интерфейс можно сконфигурировать в качестве интерфейса назначения нескольких сессий, но в качестве интерфейса источника только одной сессии.

Пример

В данном примере показано, как создать сессию мониторинга порта с номером 1, указав физический порт Ethernet 1/0/1 в качестве порта назначения, а три физических порта источника (от Ethernet 1/0/2 до Ethernet 1/0/4) в качестве портов источника.

```
Switch# configure terminal
Switch(config)#monitor session 1 destination interface ethernet 1/0/1
Switch(config)# monitor session 1 source interface ethernet 1/0/2-4
Switch(config)#
```

30.2. monitor session source interface

Данная команда используется для того, чтобы сконфигурировать порт источника (source) сессии мониторинга. Для удаления сессии мониторинга порта или порта источника из сессии из сессии мониторинга воспользуйтесь формой **no**.

monitor session *SESSION-NUMBER* **source interface {***INTERFACE-ID* **[, | -] | port-channel** *<1-8>***} [both | rx | tx]**

no monitor session *SESSION-NUMBER* **source interface** *INTERFACE-ID* **[, | -]**

no monitor session *SESSION-NUMBER*

Параметры

session *SESSION-NUMBER*	Укажите номер сессии мониторинга. Доступный диапазон значений: от 1 до 4.
interface *INTERFACE-ID*	Укажите интерфейс источника для сессии мониторинга.
,	(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.
port-channel *<1-8>*	(Опционально) Укажите агрегированную группу (Channel Group) для сессии мониторинга.
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, пакеты будут отслеживаться независимо от статуса STG на порту.

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 сессиии 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, отслеживается как TX (передаваемый), так и RX (принимаемый) 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)#
```

30.3. show monitor session

Данная команда используется для отображения указанной сессии / всех сессий мониторинга.

show monitor session [*SESSION-NUMBER***]**

Параметры

SESSION-NUMBER	(Опционально) Укажите номер сессии, которую необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

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 созданную сессию мониторинга порта с номером сессии 1.

```
Switch# show monitor session 1

Session: 1
    Session Type: local session
    Destination Port: ethernet 1/0/3
    Source Port:
        Both:
            ethernet 1/0/7
            ethernet 1/0/8
        RX:
            ethernet 1/0/9
        TX:
            ethernet 1/0/10
total entries: 1

Switch#
```

30.4. monitor session destination remote vlan

Данная команда используется для настройки RSPAN VLAN и порта назначения (destination) для сессии источника (source) RSPAN. Для удаления настроек RSPAN VLAN воспользуйтесь формой **no**.

monitor session *SESSION-NUMBER* **destination remote vlan** *VLAN-ID* **interface {***INTERFACE-ID* **| port-channel** *<1-8>***}**

no monitor session *SESSION-NUMBER* **destination remote vlan**

Параметры

SESSION-NUMBER	(Опционально) Укажите номер сессии, который необходимо отобразить.
remote vlan *VLAN-ID*	Укажите RSPAN VLAN, используемую для передачи через туннель отслеживаемых пакетов до удаленного узла.
interface *INTERFACE-ID*	Укажите интерфейс источника для сессии мониторинга порта.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду на коммутаторе источника сессии RSPAN.

Используйте команду **monitor session destination remote vlan**, чтобы сконфигурировать порт назначения, используемый для передачи отслеживаемых пакетов, и RSPAN VLAN, используемую для туннелирования отслеживаемых пакетов до удаленного узла. Порт назначения не может являться портом-участником RSPAN VLAN. В качестве порта назначения можно использовать физический порт или port-channel.

Используйте команду **monitor session source interface**, чтобы сконфигурировать порты источника, пакеты которых будут отслеживаться.

Используйте команду **remote-span** в режиме VLAN Configuration Mode, чтобы указать VLAN в качестве RSPAN VLAN. Если VLAN указана как RSPAN VLAN, связанный с этой VLAN порт access (доступ) перейдет в режим inactive. Отслеживаемые пакеты будут туннелированы через trunk-порты-участники RSPAN VLAN. RSPAN VLAN – это туннельный VLAN. Порт source (источник) не обязательно должен быть портом-участником RSPAN VLAN.

Пример

В данном примере показано, как создать сессию RSPAN на коммутаторе источника. VLAN 2 указана в качестве RSPAN VLAN, порт назначения Ethernet 1/0/2 и порт источника Ethernet 1/0/10 указаны в качестве отслеживаемых портов.

```
Switch(config)# vlan 2
Switch(config-vlan)# remote-span
Switch(config-vlan)# exit
Switch(config)# monitor session 1 destination remote vlan 2 interface ethernet
1/0/2

Switch(config)# monitor session 1 source interface ethernet 1/0/10
```

30.5. monitor session source remote vlan

Данная команда позволяет настроить RSPAN VLAN для сессии назначения (destination) RSPAN. Для удаления заданных настроек воспользуйтесь формой **no**.

monitor session *SESSION-NUMBER* **source remote vlan** *VLAN-ID*

no monitor session *SESSION-NUMBER* **source remote vlan**

Параметры

SESSION-NUMBER	(Опционально) Укажите номер сессии, который необходимо отобразить.
remote vlan *VLAN-ID*	Укажите RSPAN VLAN, используемую для передачи

	через туннель отслеживаемых пакетов до удаленного узла.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду на коммутаторе назначения сессии RSPAN.

Команда **monitor session source remote vlan** применяется для настройки VLAN, на которую туннелируются отслеживаемые пакеты источника с удаленного узла. Используйте команду monitor session destination interface, чтобы настроить порт назначения.

Используйте команду **remote-span** в режиме VLAN Configuration Mode, чтобы указать VLAN в качестве RSPAN VLAN.

Если VLAN указана как RSPAN VLAN, связанный с этой VLAN порт access (доступ), кроме интерфейса назначения, перейдет в режим inactive.

Пример

В данном примере показано, как создать сессию RSPAN на коммутаторе назначения. VLAN 100 указана в качестве RSPAN VLAN, а порт Ethernet 1/0/4 указан в качестве порта назначения. Отслеживаемые пакеты прибывают на порт Ethernet 1/0/2 и будут переданы по направлению к порту Ethernet 1/0/4.

```
Switch(config)# vlan 100
Switch(config-vlan)# remote-span
Switch(config-vlan)# exit
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 100
Switch(config-if)# exit
Switch(config)# interface ethernet 1/0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
Switch(config-if)# exit
Switch(config)# monitor session 2 source remote vlan 100
Switch(config)# monitor session 2 destination interface ethernet 1/0/4
Switch(config)#
```

31. Команды MLD Snooping

31.1. clear ipv6 mld snooping statistics

Данная команда используется для сброса счетчика статистики коммутатора.

clear ipv6 mld snooping statistics {all | vlan *VLAN-ID}*

Параметры

all	Укажите, чтобы очистить статистику IPv6 MLD Snooping для всех VLAN и портов.
vlan *VLAN-ID*	Укажите используемую VLAN. Если VLAN не указана, то очищается статистика для всех VLAN.

По умолчанию

Нет.

Режим ввода команды

Privilege EXEC Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для сброса счетчика статистики коммутатора.

Пример

В данном примере показано, как очистить всю статистику MLD Snooping.

```
Switch# clear ipv6 mld snooping statistics all
Switch#
```

31.2. ipv6 mld snooping

Данная команда используется для включения или отключения MLD Snooping.

ipv6 mld snooping

no ipv6 mld snooping

Параметры

Нет.

По умолчанию

Функция MLD Snooping отключена на всех интерфейсах VLAN.

Функция MLD Snooping отключена глобально.

Режим ввода команды

Interface Configuration Mode

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Для того, чтобы предоставить VLAN доступ к MLD 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 MLD Snooping глобально.

```
Switch# configure terminal
Switch(config)#no ipv6 mld snooping
Switch(config)#
```

В данном примере показано, как включить функцию MLD Snooping глобально.

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping
Switch(config)#
```

В данном примере показано, как включить функцию MLD Snooping на VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping
Switch(config-vlan)#
```

31.3. ipv6 mld snooping fast-leave

Данная команда используется для настройки функции MLD Snooping Fast Leave на интерфейсе. Для отключения данной функции на указанном интерфейсе воспользуйтесь формой **no**.

ipv6 mld snooping fast-leave

no ipv6 mld snooping fast-leave

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 может применяться только для настройки интерфейса VLAN. Используйте команду **ipv6 mld snooping fast-leave**, чтобы удалить членство MLD 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 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)#
```

31.4. ipv6 mld snooping last-listener-query-interval

Данная команда используется для настройки интервала, в течение которого MLD Snooping Querier отправляет сообщения Group-Specific Query (с указанием группы) или Group-Source-Specific Query (с указанием источника группы) / Channel-Source-Specific Query (с указанием источника канала). Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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, 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

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Получив сообщение MLD Done, MLD 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 listener query interval на VLAN 1000. Указанное значение – 3 секунды.

```
Switch# configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)# ipv6 mld snooping last-listener-query-interval 3
Switch(config-vlan)#
```

31.5. ipv6 mld snooping mrouter

Данная команда используется для настройки указанного интерфейса/интерфейсов в качестве router-портов, а также для указания интерфейса/интерфейсов, которые не могут быть IPv6 multicast router-портами. Для удаления интерфейса/интерфейсов из списка router-портов или списка запрещенных IPv6 multicast router-портов воспользуйтесь формой **no**.

ipv6 mld snooping mrouter {interface *INTERFACE-ID* **[,|-] | forbidden interface** *INTERFACE-ID* **[,|-]}**

no ipv6 mld snooping mrouter {interface *INTERFACE-ID* **[,|-] | forbidden interface** *INTERFACE-ID* **[,|-]}**

Параметры

interface	Укажите диапазон интерфейсов, которые подключены к многоадресным маршрутизаторам.
forbidden interface	Укажите диапазон интерфейсов, которые не подключены к многоадресным маршрутизаторам.
INTERFACE-ID	Укажите интерфейс или список интерфейсов. Пробелы до и после запятой недопустимы. В качестве интерфейса может быть использован физический порт или port-channel.

По умолчанию

По умолчанию multicast router-порты IPv6 MLD Snooping отсутствуют.

По умолчанию включено автоматическое изучение.

Режим ввода команды

Interface 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 на устройстве с MLD Snooping. При динамическом изучении устройство с MLD Snooping будет прослушивать пакеты MLD и PIMv6, для того чтобы понять, является ли подключенное к порту устройство маршрутизатором.

Пример

В данном примере показано, как настроить eth1/0/1 в качестве порта, подключенного к многоадресному маршрутизатору с MLD Snooping и eth1/0/2 в качестве порта, который не подключен к многоадресному маршрутизатору с MLD Snooping на интерфейсе 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)#
```

31.6. ipv6 mld snooping querier

Данная команда используется для включения функции MLD Snooping Querier на коммутаторе. Для отключения функции MLD Snooping Querier воспользуйтесь формой **no**.

ipv6 mld snooping querier

no ipv6 mld snooping querier

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 может применяться только для настройки интерфейса VLAN. Чтобы запустить Querier, интерфейсу необходимо присвоить IPv6-адрес.

Если система может выполнить роль Querier, устройство будет ожидать пакеты MLD Query, отправленные другими устройствами. При получении сообщения MLD Query устройство с более низким значением IPv6-адреса становится Querier.

Пример

В данном примере показано, как включить MLD Snooping Querier на VLAN 1.

```
Switch# configure terminal
Switch(config)#vlan 1
Switch(config-vlan)# ipv6 mld snooping querier
Switch(config-vlan)#
```

31.7. ipv6 mld snooping query-interval

Данная команда используется для настройки интервала между сообщениями MLD General Query. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

ipv6 mld snooping query-interval *SECONDS*

no ipv6 mld snooping query-interval

Параметры

SECONDS	Укажите интервал между сообщениями MLD General Query для обозначенного маршрутизатора. Доступный диапазон значений: от 1 до 31744.

По умолчанию

Значение по умолчанию – 125 секунд.

Режим ввода команды

Interface 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 MLD-сообщений, изменяя значение данного интервала: 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)#
```

31.8. ipv6 mld snooping query-max-response-time

Данная команда используется для настройки максимального значения времени ожидания, анонсированного в сообщениях MLD Snooping Query. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

ipv6 mld snooping query-max-response-time *SECONDS*

no ipv6 mld snooping query-max-response-times

Параметры

SECONDS	Укажите максимальное значение времени ожидания, анонсированное в сообщениях MLD Snooping Query. Доступный диапазон значений: от 1 до 25 секунд.

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

Interface 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 MLD Query, прежде чем его участие будет удалено посредством MLD Snooping.

Пример

В данном примере показано, как настроить максимальное значение времени ожидания на VLAN 1000. Указанное значение – 20 секунд.

```
Switch# configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)# ipv6 mld snooping query-max-response-time 20
Switch(config-vlan)#
```

31.9. ipv6 mld snooping query-version

Данная команда используется для настройки версии пакетов General Query, отправляемых MLD Snooping Querier. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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. Указанная версия – 1.
2	Укажите версию пакета MLD General Query, отправленного MLD Snooping Querier. Указанная версия – 2.

По умолчанию

Значение по умолчанию – 2.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN.

Пример

В данном примере показано, как настроить версию пакета 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)#
```

31.10. ipv6 mld snooping robustness-variable

Данная команда используется для настройки robustness variable (переменной надежности), используемой в MLD Snooping. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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

Interface 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 MLD-сообщений:

- **Group member interval** – промежуток времени, по истечении которого многоадресный 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)# ipv6 mld snooping robustness-variable 3
Switch(config-vlan)#
```

31.11. ipv6 mld snooping static-group

Данная команда используется для настройки статической группы MLD Snooping. Для удаления статической группы воспользуйтесь формой **no**.

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 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

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Используйте данную команду на интерфейсе VLAN, чтобы добавить запись статической группы.

Используйте команду **ipv6 mld snooping static-group**, чтобы создать статическую группу MLD Snooping, если подключенный узел не поддерживает MLD-протокол.

Пример

В данном примере показано, как добавить запись статической группы для MLD Snooping на VLAN 1.

```
Switch# configure terminal
Switch(config)#vlan 1
Switch(config-vlan)# ipv6 mld snooping static-group FF02::12:03 interface ethernet
1/0/5
Switch(config-vlan)#
```

31.12. show ipv6 mld snooping

Данная команда используется для отображения информации о 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

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию об MLD Snooping для всех VLAN, на которых включена данная функция, не указывая определенную VLAN.

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
  Fast leave            : Enabled (host-based)
  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#
```

31.13. 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 IPv6-адрес группы. Если IPv6-адрес не указан, будет отображена информация обо всех группах MLD .
vlan *VLAN-ID*	(Опционально) Укажите интерфейс VLAN. Если интерфейс не указан, будет отображена информация о группе MLD Snooping для всех интерфейсов.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

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       Exp(sec)  Interface
-------  -------------------  -------------------  --------  ---------
1        FF1E::                        *           258       2/0/7
1        FF1E::3                       *           258       2/0/7
1        FF1E::4              3620:110:1::3a2b     258       2/0/7

Total Entries: 3

Switch#
```

31.14. show ipv6 mld snooping mrouter

Данная команда используется для отображения информации о multicast router-порте MLD Snooping, который был автоматически изучен и настроен вручную на коммутаторе.

show ipv6 mld snooping mrouter [vlan *VLAN-ID***]**

Параметры

VLAN-ID	(Опционально) Укажите VLAN. 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

Любой режим конфигурирования

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 MLD Snooping.

```
Switch# show ipv6 mld snooping mrouter

VLAN   Ports
-----  -----------------------------
4094   1/0/12 (forbidden)

Total Entries: 3

Switch#
```

31.15. show ipv6 mld snooping static-group

Данная команда используется для отображения статически настроенной группы MLD Snooping на коммутаторе.

show ipv6 mld snooping static-group [*GROUP-ADDRESS* **| vlan** *VLAN-ID***]**

Параметры

GROUP-ADDRESS	Укажите IPv6-адрес группы, которую необходимо отобразить.
vlan *VLAN-ID*	Укажите VLAN ID, который необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить статически настроенную группу MLD Snooping.

Пример

В данном примере показано, как отобразить статически настроенную группу MLD Snooping.

```
Switch#show ipv6 mld snooping static-group

VLAN ID  Group address                          Interface
-------  ---------------                        -------------------------
1        FF1E::1                                1/0/1,1/0/5

Total Entries: 1

Switch#
```

31.16. show ipv6 mld snooping statistics

Данная команда используется для отображения информации о статистике MLD Snooping на коммутаторе.

show ipv6 mld snooping statistics vlan [*VLAN-ID***]**

Параметры

vlan *VLAN-ID*	Укажите VLAN ID для отображения статистики MLD Snooping.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию о статистике MLD Snooping.

Пример

В данном примере показано, как отобразить информацию о статистике MLD Snooping.

```
Switch# show ipv6 mld snooping statistics vlan

VLAN1 Statistics:
Rx: v1Report 0, v2Report 58, Query 0, v1Done 0
Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Total Entries: 1

Switch#
```

32. Команды Multiple Spanning Tree Protocol (MSTP)

32.1. 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

INSTANCE-ID	Укажите ID MSTP-экземпляра, к которому необходимо привязать указанные VLAN. Доступный диапазон значений: от 1 до 4094.
vlans *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.

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)#
```

32.2. 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)#
```

32.3. 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)#
```

32.4. show spanning-tree mst

Данная команда используется для отображения информации, которая использовалась в версии MSTP.

show spanning-tree mst [configuration]

show spanning-tree mst [instance *INSTANCE-ID* **[, | -]] [interface** *INTERFACE-ID* **[, | -]] [detail]**

Параметры

configuration	Укажите, чтобы отобразить таблицу соотношений между несколькими VLAN и экземплярами MSTP.
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-ID*	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

Любой режим конфигурирования

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)

 ethernet 1/0/1
   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 ethernet 1/0/1 detail

ethernet 1/0/1
 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#
 ---------      ----       -----      ----      -------
 ethernet 1/0/1       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 ethernet 1/0/3-4

ethernet 1/0/3
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

ethernet 1/0/4
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 ethernet 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#
---------  ----       -----      ------  ---------
ethernet 1/0/3    backup     blocking   200000    128.3
ethernet 1/0/4    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#
```

32.5. 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-ID	Укажите ID MSTP-экземпляра.
cost *COST*	Укажите стоимость пути экземпляра. Доступный диапазон значений: от 0 до 200000000.
port-priority *PRIORITY*	Укажите приоритет порта экземпляра. Доступный 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 ethernet 1/0/1
Switch(config-if)# spanning-tree mst 0 cost 17031970
Switch(config-if)#
```

32.6. 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)#
```

32.7. 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)#
```

32.8. 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, чтобы определить интервал времени 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 ethernet 1/0/1
Switch(config-if)# spanning-tree mst hello-time 1
Switch(config-if)#
```

32.9. 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)#
```

33. Команды Network Access Authentication

33.1. authentication guest-vlan

Данная команда используется для настройки Guest VLAN. Для удаления Guest VLAN воспользуйтесь формой **no**.

authentication guest-vlan *VLAN-ID*

no authentication guest-vlan

Параметры

VLAN-ID	Укажите Guest VLAN для аутентификации.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда не может быть использована, если указанная VLAN не существует в качестве статической VLAN. Узел не может получить доступ к сети, пока не пройдет аутентификацию. Если Guest VLAN настроена, узлу разрешается доступ только к Guest VLAN без прохождения аутентификации. Во время аутентификации, если RADIUS-сервер назначает пользователю VLAN, пользователь будет авторизован в назначенной VLAN. Назначение Guest VLAN и VLAN не действует на порт trunk VLAN и порт tunnel VLAN.

Обычно назначение Guest VLAN и VLAN действует для узлов, подключенных к нетегированным портам. Данный функционал не применим в случае, если узлы обмениваются тегированным трафиком.

Если режим узла (host mode) аутентификации настроен как **multi-host**, порт будет добавлен как Guest VLAN порт, а PVID порта будет изменен на Guest VLAN. Трафик, приходящий из Guest VLAN, будет перенаправлен независимо от аутентификации. Трафик, приходящий от других VLAN, будет отбрасываться, пока не пройдет аутентификацию. Когда один узел проходит аутентификацию, порт покидает Guest VLAN и будет добавлен в назначенную VLAN. PVID порта будет изменен на назначенную VLAN.

Если режим узла (host mode) аутентификации настроен как **multi-auth**, порт будет добавлен как Guest VLAN порт, и PVID порта будет изменен на Guest VLAN. Узлам, которым разрешен доступ к Guest VLAN, запрещен доступ к другим VLAN, пока они не пройдут аутентификацию. Когда один узел проходит аутентификацию, порт остается в Guest VLAN, а PVID порта не изменяется.

Если Guest VLAN отключена, порт выйдет из Guest VLAN и вернется к родной VLAN (native). PVID изменится на PVID родной VLAN.

Пример

В данном примере показано, как указать VLAN 5 в качестве Guest VLAN.

```
Switch# configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)# authentication guest-vlan 5
Switch(config-if)#
```

33.2. authentication host-mode

Данная команда используется для указания режима аутентификации. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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) 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 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 блокироваться на период молчания (quiet period). Порт восстановит обработку пакетов EAPOL после периода молчания.

Если порт работает в режиме **multi-auth**, каждый узел должен проходить аутентификацию индивидуально для доступа к порту. Узел представлен своим MAC-адресом. Доступ есть только у авторизованных узлов.

Пример

В данном примере показано, как назначить режим multi-host для 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)#
```

33.3. authentication periodic

Данная команда используется для включения периодического повторения аутентификации для порта. Для отключения периодического повторения аутентификации воспользуйтесь формой **no**.

authentication periodic

no authentication periodic

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 включить периодическое повторение аутентификации для порта.

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)#
```

33.4. authentication timer reauthentication

Данная команда используется для настройки таймера, по истечении которого будет необходимо пройти повторную аутентификацию. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

authentication timer reauthentication {*SECONDS***}**

no authentication timer reauthentication

Параметры

SECONDS	Укажите время, после которого будет необходимо пройти повторную аутентификацию. Доступный 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 данную команду, чтобы настроить таймер, по истечении которого будет необходимо пройти повторную аутентификацию.

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)#
```

33.5. authentication timer restart

Данная команда используется для настройки таймера, по истечении которого станет возможна повторная аутентификация после последней неудачной попытки. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

authentication timer restart *SECONDS*

no authentication timer restart

Параметры

SECONDS	Укажите время, по истечении которого станет возможна повторная аутентификация. Доступный диапазон значений: 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)#
```

33.6. authentication username

Данная команда используется для создания пользователя в локальной базе данных аутентификации. Для удаления пользователя из локальной базы данных аутентификации воспользуйтесь формой **no**.

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) Укажите пароль в обычном текстовом виде. Если не указан ни 0, ни 7, по умолчанию паролем будет обычный текст.
7	(Опционально) Укажите зашифрованный пароль. Если не указан ни 0, ни 7, по умолчанию паролем будет обычный текст.
password *STRING*	Укажите, чтобы задать пароль для MAC-аутентификации. Если указан пароль в обычном текстовом виде, длина строки не может превышать 32 символа.
vlan *VLAN-ID*	Укажите, чтобы назначить VLAN.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode

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)#
```

33.7. clear authentication sessions

Данная команда используется для удаления сессий аутентификации.

clear authentication sessions {dot1x | all | interface *INTERFACE-ID* **[dot1x] | mac-address** *MAC-ADDRESS***}**

Параметры

dot1x	Укажите для удаления всех сессий dot1x.
all	Укажите для удаления всех сессий.
interface *INTERFACE-ID*	Укажите для удаления сессий порта.
mac-address *MAC-ADDRESS*	Укажите для удаления всех сессий определенного пользователя.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы удалить сессии аутентификации.

Пример

В данном примере показано, как удалить сессии аутентификации на порту Ethernet 1/0/1.

```
Switch# clear authentication sessions interface ethernet 1/0/1
Switch#
```

33.8. authentication mac-move deny

Данная команда используется для отключения MAC move на коммутаторе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

authentication mac-move deny

no authentication mac-move deny

Параметры

Нет.

По умолчанию

По умолчанию данная функция разрешена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда определяет, разрешать ли аутентифицированным узлам перемещаться по различным портам коммутатора. Данная команда позволяет настроить управление таким образом, чтобы только узлу, аутентифицированному на порту в режиме **multi-auth**, было разрешено перемещаться к другому порту.

Если узлу разрешено перемещаться, то возможны две ситуации. Он может быть либо повторно аутентифицирован, либо он напрямую переместится на новый порт без повторной аутентификации на основе следующего правила. Если новый порт имеет ту же настройку аутентификации, что и оригинальный (исходный) порт, повторная аутентификация не требуется. Узел наследует те же атрибуты авторизации для нового порта. Аутентифицированный узел может перемещаться от порта 1 к порту 2 с теми же атрибутами авторизации без необходимости повторной аутентификации. Если настройки аутентификации нового порта отличаются от настроек оригинального порта, то требуется повторная аутентификация. Аутентифицированный узел на порту 1 может переместиться и быть повторно аутентифицированным на порту 2. Если на новом порту не включен метод аутентификации, то узел напрямую может переместиться на него. Сессия с оригинальным портом будет удалена. Аутентифицированный узел будет перемещен с порта 1 на порт 2.

Если функция MAC move отключена, и аутентифицированный узел перемещается на другой порт, это расценивается как нарушение правила.

Пример

В данном примере показано, как включить MAC move на коммутаторе.

```
Switch# configure terminal
Switch(config)#authentication mac-move deny
Switch(config)#
```

33.9. authorization disable

Данная команда используется для отключения приема авторизованной конфигурации. Для включения приема авторизованной конфигурации воспользуйтесь формой **no**.

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 принятия авторизованной конфигурации. Если авторизация включена для аутентификации, авторизованные атрибуты (например, VLAN, приоритет 802.1p по умолчанию, Bandwidth (полоса пропускания) и ACL (список управления доступом), назначенные RADIUS-сервером, будут приняты, если включено состояние авторизации. Bandwidth (полоса пропускания) и ACL (список управления доступом) назначаются на основе порта. В режиме **multi-auth** VLAN и 802.1p назначаются на основе узла.

Пример

В данном примере показано, как включить состояние авторизации.

```
Switch# configure terminal
Switch(config)#no authorization disable
Switch(config)#
```

33.10. show authentication sessions

Данная команда используется для просмотра информации об аутентификации.

show authentication sessions [dot1x | interface *INTERFACE-ID* **[, | -] [dot1x] | mac-address** *MAC-ADDRESS***]**

Параметры

dot1x	(Опционально) Укажите для отображения всех сессий dot1x.
interface *INTERFACE-ID*	(Опционально) Укажите порт для отображения.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

mac-address *MAC-ADDRESS*	(Опционально) Укажите для отображения определенного пользователя.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду без параметров, чтобы включить отображение сессий со всех портов.

Пример

В данном примере показано, как включить отображение сессий на порту Ethernet 1/0/1.

```
Switch# show authentication sessions interface ethernet 1/0/1

Interface: ethernet 1/0/1
MAC Address: 00-16-76-35-1A-38
Authentication VLAN: 1

Authentication Username: Administrator
Assigned Priority: 0
Assigned Ingress Bandwidth : 0 kbps
Assigned Egress Bandwidth  : 0 kbps
802.1X Authenticator State: HELD
802.1X Backend State : IDLE


Total Authenticating Hosts: 0
Total Authenticated Hosts: 1
Total Blocked Hosts: 0

Switch#
```

Отображаемые параметры

Interface	Принимающий интерфейс узла аутентификации.
MAC Address	MAC-адрес узла аутентификации.
Authentication VLAN	Исходная VLAN начала аутентификации узла.

Authentication State	Состояние аутентификации узла. **Start** – принимается узел, но не было начала аутентификации **Initialization** – источник аутентификации готов, но новая аутентификация не начинается **Authenticating** – узел проходит аутентификацию **Failure** – ошибка аутентификации **Success** – узел прошел аутентификацию
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 или JWAC.
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, JWAC 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 не

	аутентифицированное 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 установить подключение с запрашивающим устройством. **AUTHENTICATING** – запрашивающее устройство проходит аутентификацию. **AUTHENTICATED** – аутентификатор успешно аутентифицировал запрашивающее устройство. **ABORTING** – процедура аутентификации преждевременно отменена из-за запроса на повторную авторизацию, кадра EAPOL-Start, EAPOL-Logoff или тайм-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.

34. Команды Port Security

34.1. clear port-security

Данная команда позволяет удалить автоматически изученные безопасные MAC-адреса.

clear port-security {all | {address *MAC-ADDR* **| interface** *INTERFACE-ID* **[, | -]}}**

Параметры

all	Укажите, чтобы удалить все автоматически изученные безопасные MAC-адреса.
address MAC-ADDR	Укажите, чтобы удалить указанные автоматически изученные безопасные записи на основе введенного MAC-адреса.
interface *INTERFACE-ID*	Укажите, чтобы удалить все автоматически изученные безопасные записи на указанном интерфейсе.
,	(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

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#
```

34.2. show port-security

Данная команда используется для просмотра текущих настроек Port Security.

show port-security [[[interface *INTERFACE-ID* **[, | -]] | [address]]**

Параметры

INTEFACE-ID	Укажите ID интерфейса, который необходимо отобразить.
,	Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
address	Укажите для отображения безопасных MAC-адресов, включая настроенные и изученные адреса.

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 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
Interface No.    : ethernet 1/0/1
Max No.          : 32
Curr No.         : 0
Violation Action : Protect
Violation Count  : -
Security Mode    : DeleteOnTimeout
Admin State      : Disabled
Current State    : -
Aging Time       : 0
Aging Type       : Absolute

Interface No.    : ethernet 1/0/2
Max No.          : 32
Curr No.         : 0
Violation Action : Protect
Violation Count  : -
Security Mode    : DeleteOnTimeout
Admin State      : Disabled
Current State    : -
Aging Time       : 0
Aging Type       : Absolute

Interface No.    : ethernet 1/0/3
Max No.          : 32
Curr No.         : 0
Violation Action : Protect
Violation Count  : -
Security Mode    : DeleteOnTimeout
Admin State      : Disabled
Current State    : -
Aging Time       : 0
Aging Type       : Absolute

Switch#
```

34.3. snmp-server enable traps port-security

Данная команда используется для включения отправки SNMP-уведомлений при обнаружении функционалом Port Security недопустимых адресов. Для отключения отправки SNMP-уведомлений воспользуйтесь формой **no**.

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. Доступный диапазон значений: от 0 до 1000. Значение по умолчанию 0 означает, что SNMP-трап будет генерироваться для каждого нарушения безопасности.

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 или отключить отправку SNMP-уведомлений при обнаружении функционалом Port Security недопустимых адресов, а также, чтобы настроить количество трапов в секунду.

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
Switch(config)# snmp-server enable traps port-security trap-rate 3
Switch(config)#
```

34.4. switchport port-security

Данная команда используется для настройки параметров Port Security, чтобы ограничить количество пользователей, которым разрешен доступ к порту. Для отключения Port Security или удаления безопасного MAC-адреса воспользуйтесь формой **no**.

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. Доступный 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 данная 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), JWAC, 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 интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)# switchport port-security mac-address 00-00-12-34-56-78 vlan 5
Switch(config-if)#
```

В 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)#
```

34.5. switchport port-security aging

Данная команда позволяет задать время старения (aging time) для динамически изученных безопасных адресов на интерфейсе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

switchport port-security aging {time *MINUTES* **| type {absolute | inactivity}}**

no switchport port-security aging {time | type}

Параметры

MINUTES	Укажите время старения (aging time) для динамически изученных безопасных адресов на порту в минутах. Доступный диапазон значений: 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 данная 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

Используйте данную команду, чтобы отключить процесс 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 интерфейса Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)# switchport port-security aging time 1
Switch(config-if)#
```

В данном примере показано, как настроить тип времени старения для интерфейса 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)#
```

34.6. port-security limit

Данная команда позволяет задать максимальное количество безопасных MAC-адресов в системе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

port-security limit global *VALUE*

no port-security limit global

Параметры

VALUE	Укажите максимальное число записей Port Security, которое может быть изучено в системе. Доступный диапазон значений: от 1 до 6656. Если указанное значение меньше текущего числа изученных записей, команда будет отклонена.

По умолчанию

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.

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)#
```

34.7. show port-security global-settings

Данная команда используется для отображения глобальных настроек Port Security.

show port-security global-settings

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить глобальные настройки Port Security.

Пример

В данном примере показано, как отобразить глобальные настройки Port Security.

```
Switch# show port-security global-settings
Trap State             : Disabled
Trap Rate              : 0
System Maximum Address : No Limit

Switch#
```

34.8. show snmp-server traps port-security

Данная команда используется для отображения состояния трапов Port Security.

show snmp-server traps port-security

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить состояние трапов Port Security.

Пример

В данном примере показано, как отобразить состояние трапов Port Security.

```
Switch# show snmp-server traps port-security
  port-security              : Disabled
Switch#
```

35. Команды энергосбережения

35.1. dim led

Данная команда используется для отключения индикаторов портов с целью энергосбережения. Для того чтобы не отключать индикаторы портов с целью энергосбережения воспользуйтесь формой **no**.

dim led

no dim led

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 отключить индикаторы портов с целью энергосбережения. Для того чтобы не отключать индикаторы портов с целью энергосбережения воспользуйтесь формой **no**. 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)#
```

35.2. power-saving

Данная команда используется для включения отдельных функций энергосбережения. Для отключения данной функции воспользуйтесь формой **no**.

power-saving {port-shutdown | dim-led | hibernation}

no power-saving {port-shutdown | dim-led | hibernation}

Параметры

dim-led	Укажите, чтобы включать функцию энергосбережения по расписанию отключения индикаторов.
port-shutdown	Укажите, чтобы включать функцию энергосбережения по расписанию отключения порта.
hibernation	Укажите, чтобы включать функцию энергосбережения по расписанию режима сна системы. Этот параметр можно использовать только в том случае, если стекирование отключено.

По умолчанию

По умолчанию все функции отключены.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы включить или отключить индикаторы, отключить порт, перейти в режим сна.

При включении **dim LED** устройство выключит все индикаторы порта в указанном временном диапазоне для экономии энергии.

При включении **port shutdown** устройство отключит все порты в указанном временном диапазоне для экономии энергии.

При включении **hibernation** устройство перейдет в режим сна в указанном временном диапазоне для экономии энергии. Этот параметр можно использовать только в том случае, если стекирование отключено.

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)#
```

35.3. power-saving dim-led time-range

Данная команда используется для настройки профиля временного диапазона для расписания отключения индикаторов (Dim LED). Для удаления указанного профиля временного диапазона воспользуйтесь формой **no**.

power-saving dim-led time-range *PROFILE-NAME*

no power-saving dim-led time-range *PROFILE-NAME*

Параметры

PROFILE-NAME	Укажите имя настраиваемого профиля временного диапазона. 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)#
```

35.4. power-saving hibernation time-range

Данная команда используется для настройки профиля временного диапазона для расписания режима сна системы (Hibernation). Для удаления профиля временного диапазона воспользуйтесь формой **no**.

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. Этот параметр можно использовать только в том случае, если стекирование отключено.

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)#
```

35.5. power-saving shutdown time-range

Данная команда используется для настройки профиля временного диапазона для расписания отключения порта (Port Shutdown). Для удаления профиля временного диапазона воспользуйтесь формой **no**.

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)#
```

35.6. show power-saving

Данная команда используется для отображения информации о настройках энергосбережения.

show power-saving [dim-led] [port-shutdown] [hibernation]

Параметры

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.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

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 обо всех настройках энергосбережения.

```
Switch#show power-saving
Function Version: 3.00

Scheduled Hibernation  power saving
  State: Disable

Administrative Dim-LED
  State: Disabled

Scheduled Dim-LED Power Saving
  State: Disabled

Scheduled Port-shutdown Power Saving
  State: Disabled

Switch#
```

36. Команды Protocol Independent

36.1. ip route

Данная команда используется для создания записи статического маршрута. Для удаления записи статического маршрута воспользуйтесь формой **no**.

ip route *NETWORK-PREFIX NETWORK-MASKIP-ADDRESS* **[primary | backup]**

no ip route *NETWORK-PREFIX NETWORK-MASKIP-ADDRESS*

Параметры

NETWORK-PREFIX	Укажите сетевой адрес.
NETWORK-MASK	Укажите сетевую маску.
IP-ADDRESS	Укажите IP-адрес следующего узла (Next Hop), который может быть использован 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

Используйте данную команду, чтобы создать IP статического маршрута. 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)#
```

36.2. ipv6 route

Данная команда используется для создания записи статического маршрута IPv6. Для удаления записи статического маршрута IPv6 воспользуйтесь формой **no**.

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 пакета.
NEXT-HOP-ADDRESS	(Опционально) 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 одним

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)#
```

36.3. 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) Укажите, чтобы отобразить подключенный маршрут.
static	(Опционально) Укажите, чтобы отобразить статический маршрут.
hardware	(Опционально) Укажите, чтобы отобразить маршруты, которые были записаны на чип.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить самые приоритетные маршруты, которые являются текущей записью маршрута.

Пример

В данном примере показано, как отобразить таблицу маршрутизации.

```
Switch#show ip route
Code: C - connected, S - static
      * - candidate default


Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, vlan1

Total Entries: 1


Switch#
```

36.4. 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

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить краткую информацию 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#
```

36.5. show ipv6 route

Данная 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) Укажите, чтобы отобразить маршрут и все указанные маршруты.
INTERFACE-ID	(Опционально) Укажите тип интерфейса.
connected	(Опционально) Укажите, чтобы отобразить подключенный маршрут.
static	(Опционально) Укажите, чтобы отобразить статический маршрут.
database	(Опционально) Укажите, чтобы отобразить все связанные записи в базе данных маршрутизации, а не только самый приоритетный маршрут.
hardware	(Опционально) Укажите, чтобы отобразить маршруты, которые были записаны на чип.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить самые приоритетные маршруты, которые являются текущей записью маршрута.

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, как отобразить записи 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#
```

36.6. 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

Любой режим конфигурирования

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          0
Total           3
Switch#
```

37. Команды Quality of Service (QoS)

37.1. mls qos cos

Данная команда используется для настройки значения Class of Service (CoS) по умолчанию для порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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

По умолчанию значение CoS – 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**, когда все входящие пакеты на определенных портах заслуживают приоритет выше или ниже, чем пакеты, поступающие из других портов. При использовании данной команды, ранее настроенные доверенные DSCP и CoS будут перезаписаны, и все значения CoS входящих пакетов будут изменены на CoS по умолчанию, настроенный в команде **mls qos cos**. Если входящие пакеты тегированные, их значение CoS изменяется на входном порту.

Пример

В данном примере показано, как настроить значение COS по умолчанию на 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)#
```

37.2. mls qos map dscp-cos

Данная команда используется для привязки DSCP-меток к CoS. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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 командой **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)#
```

37.3. mls qos scheduler

Данная команда используется для настройки механизма обслуживания очередей. Для сброса механизма обслуживания очередей пакетов к значению по умолчанию воспользуйтесь формой **no**.

mls qos scheduler {sp | wrr }

no mls qos scheduler

Параметры

sp	Укажите алгоритм Strict Priority, SP 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.

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 или SP) для выходной очереди. Алгоритм обслуживания очередей для очереди по умолчанию – WRR.

WRR предназначен для передачи разрешенных пакетов в очереди передачи в режиме Round-Robin. Изначально вес каждой очереди установлен на основе настроенного веса. Каждый раз, когда пакет отправляется из очереди CoS с более высоким приоритетом, из соответствующего веса вычитается 1, и право на обслуживание переходит к пакету из очереди CoS с приоритетом ниже предыдущего. Если вес очереди CoS достигает нуля, очередь не обслуживается до тех пор, пока ее вес не будет возобновлен. Вес всех очередей CoS при достижении нуля возобновляется за один раз.

Пример

В данном примере показано, как настроить алгоритм обслуживания очередей в режиме Strict Priority.

```
Switch# configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)# mls qos scheduler sp
Switch(config-if)#
```

37.4. mls qos trust

Данная команда используется для настройки доверенного статуса (Trust) на порту для поля CoS или DSCP поступающего пакета для последующих QoS-операций. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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-cos**. Чтобы настроить CoS в карте очереди, используйте команду **priority-queue cos-map**. Если приходящий пакет не IP-пакет, доверенным будет CoS. В передаваемом пакете также будет CoS, полученный в результате привязки DSCP.

После настройки статуса Trust для CoS на интерфейсе, CoS приходящих пакетов будет применен в качестве внутреннего CoS и использован для определения очереди CoS. Очередь CoS определяется на основе таблицы соответствия CoS и очереди.

Пакету, прибывшему на порт 802.1Q VLAN tunnel, будет добавлен внешний тег VLAN для передачи через VLAN tunnel. Если на порту настроен статус Trust для CoS, тег внутреннего CoS будет являться CoS пакета и значением CoS во внешнем теге VLAN пакета. Если при вводе команды **mls qos cos** был указан параметр **override**, то внутренним CoS пакета и значением CoS во внешнем теге VLAN пакета будет CoS, настроенный в команде **mls qos cos**. Если на порту настроен статус Trust для DSCP, то внутренним CoS пакета и значением CoS во внешнем теге VLAN пакета будет CoS, полученный в результате привязки DSCP.

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)#
```

37.5. priority-queue cos-map

Данная команда используется для привязки CoS к карте очереди. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

37.6. queue rate-limit

Данная команда используется для указания или изменения полосы пропускания, предназначенной для очереди. Для удаления полосы пропускания, предназначенной для очереди воспользуйтесь формой **no**.

queue *QUEUE-ID* **rate-limit {***MIN-BANDWIDTH-KBPS MAX-BANDWIDTH-KBPS* **| percent** *MIN-PERCENTAGE 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, чтобы установить минимальную полосу пропускания в процентах. Доступный диапазон значений: от 1 до 100.
MAX-PERCENTAGE	Укажите, чтобы установить 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 50
Switch(config-if)#
```

37.7. rate-limit {input | output}

Данная команда используется для настройки ограничения полосы пропускания для входящего либо исходящего трафика на интерфейсе. Для отмены ограничения полосы пропускания трафика воспользуйтесь формой **no**.

rate-limit {input | output} {*NUMBER-KBPS* **| percent** *PERCENTAGE***}**

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.

По умолчанию

По умолчанию ограничения не установлены.

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)#
```

37.8. show mls qos interface

Данная команда используется для отображения настроек уровня QoS на указанном интерфейсе.

show mls qos {interface *INTERFACE-ID* **[, | -] | dscp-cos-map} {cos | scheduler | trust | rate-limit | queue-rate-limit }**

Параметры

interface *INTERFACE-ID*	Укажите interface ID, 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.
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 ограничения полосы пропускания, настроенной для порта.
queue-rate-limit	Укажите, чтобы отобразить ограничение полосы пропускания, настроенной для очереди.
dscp-cos-map	Укажите, чтобы отобразить привязку DSCP к CoS.

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 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 eth 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 eth 1/0/2-5 trust

Interface   Trust State
----------- ------------
eth1/0/2     trust DSCP
eth1/0/3     trust CoS
eth1/0/4     trust DSCP
eth1/0/5     trust CoS

Switch#
```

В 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 eth 1/0/1-2 scheduler

Interface   Scheduler Method
----------  ------------------
eth1/0/1      sp
eth1/0/2      wrr

Switch#
```

В данном примере показано, как отобразить ограничение полосы пропускания на портах с 1/0/1 по 1/0/4.

```
Switch# show mls qos interface eth 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 eth 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 привязку DSCP к CoS для интерфейса Ethernet 1/0/1.

```
Switch# show mls qos interface ethernet 1/0/1 dscp-cos-map

eth1/0/1
CoS    DSCP List
----   ----------
0      0-7
1      8-15
2      16-23
3      24-31
4      32-39
5      40-47
6      48-55
7      56-63
Switch#
```

37.9. 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

Любой режим конфигурирования

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 queuing

 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 queuing interface ethernet 1/0/3

wrr bandwidth weights:
  CoS   Weights
  ---  -------
   0      1
   1      2
   2      3
   3      4
   4      5
   5      6
   6      7
   7      8

Switch#
```

37.10. wdrr-queue bandwidth

Данная команда используется для настройки значений Quantum для очередей, обслуживаемых механизмом WDRR. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

wdrr-queue bandwidth *QUANTUM1…QUANTUM127*

no wdrr-queue bandwidth

Параметры

QUANTUM1…QUANTUM127	Укажите значение Quantum (число длины кадров) для каждой очереди, обслуживаемой механизмом WDRR.

По умолчанию

Нет.

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 значение 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 eth 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)#
```

37.11. wrr-queue bandwidth

Данная команда используется для настройки веса (Weight) для очередей, обслуживаемых механизмом WRR. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

wrr-queue bandwidth *WEIGHT1…WEIGHT127*

no wrr-queue bandwidth

Параметры

WEIGHT1…WEIGHT127	Укажите значение веса (число кадров) для каждой очереди, обслуживаемой механизмом WRR.

По умолчанию

Нет.

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)#
```

38. Команды Remote Network MONitoring (RMON)

38.1. rmon collection stats

Данная команда используется для включения статистики RMON на настраиваемом интерфейсе. Для отключения статистики RMON воспользуйтесь формой **no**.

rmon collection stats *INDEX* **[owner** *NAME***]**

no rmon collection stats *INDEX*

Параметры

INDEX	Укажите индекс таблицы Remote Network Monitoring (RMON). Доступный диапазон значений: от 1 до 65535.
owner *NAME*	Укажите строку владельца. Максимально допустимое количество символов в строке – 127 символов.

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)#
```

38.2. rmon collection history

Данная команда используется для включения сбора истории статистики RMON MIB на настраиваемом интерфейсе. Для отключения сбора истории статистики на интерфейсе воспользуйтесь формой **no**.

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 символов.
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 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)#
```

38.3. rmon alarm

Данная команда используется для настройки записи уровня alarm (тревога) для мониторинга интерфейса. Для удаления записи уровня alarm воспользуйтесь формой **no**.

rmon alarm *INDEX VARIABLE INTERVAL* **{delta | absolute} rising-threshold** *VALUE* **[***RISING-EVENT-NUMBER***] falling-threshold** *VALUE* **[***FALLING-EVENT-NUMBER***] [owner** *STRING***]**

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 на 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*	Укажите строку владельца. Максимально допустимая длина – 127 символов.

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)#
```

38.4. rmon event

Данная команда используется для настройки записи события. Для удаления записи события воспользуйтесь формой **no**.

rmon event *INDEX* **[log] [trap** *COMMUNITY***] [owner** *NAME***] [description** *STRING***]**

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. Максимальная длина – 127 символов.
owner *NAME*	(Опционально) Укажите имя владельца. Максимальная длина – 127 символов.
description *STRING*	(Опционально) Укажите описание для записи события RMON. Максимально допустимое количество символов в строке – 127 символов.

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)#
```

38.5. 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

Любой режим конфигурирования

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#
```

38.6. 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

Любой режим конфигурирования

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, 2014-03-12

Event 2, owned by manager2
  Description is Errors
  Event trigger action: log & trap
  Last triggered time:

Switch#
```

38.7. 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

Любой режим конфигурирования

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 ethernet 1/0/2
  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#
```

38.8. 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

Любой режим конфигурирования

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 ethernet 1/0/3
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#
```

38.9. snmp-server enable traps rmon

Данная команда используется для включения отправки 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 отправку RMON trap.

Пример

В данном примере показано, как включить отправку RMON trap, уведомляющих о поднятии и об отмене тревоги.

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

38.10. show snmp-server traps rmon

Данная команда используется для отображения RMON trap.

show snmp-server traps rmon

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить RMON trap.

Пример

В данном примере показано, как отобразить RMON trap.

```
Switch# show snmp traps rmon

Rmon Trap State:
    RMON Rising Alarm Trap: Enabled
    RMON Falling Alarm Trap: Enabled

Switch#
```

39. Команды Safeguard Engine

39.1. cpu-protect safeguard

Данная команда используется для включения или настройки функции Safeguard Engine. Для отключения функции Safeguard Engine воспользуйтесь формой **no**.

cpu-protect safeguard

no cpu-protect safeguard

Параметры

Нет.

По умолчанию

По умолчанию функция Safeguard Engine отключена.

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.

Пример

В данном примере показано, как включить функцию Safeguard Engine.

```
Switch# configure terminal
Switch(config)#cpu-protect safeguard
Switch(config)#
```

39.2. 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

Любой режим конфигурирования

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

Switch#
```

40. Команды Secure Sockets Layer (SSL)

40.1. show ssl-service-policy

Данная команда используется для отображения политики SSL Service Policy.

show ssl-service-policy [*POLICY-NAME***]**

Параметры

POLICY-NAME	(Опционально) Укажите имя политики SSL Service Policy.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если имя политики SSL Service Policy не указано, отобразятся все SSL Service Policy.

Пример

В данном примере показано, как отобразить все SSL Service Policy.

```
Switch# show ssl-service-policy

SSL Policy Name        : policy1
  Enabled Cipher Suites:
    RSA_WITH_RC4_128_MD5,
    RSA_WITH_3DES_EDE_CBC_SHA,
    RSA_EXPORT_WITH_RC4_40_MD5
  Session Cache Timeout: 600

SSL Policy Name        : policy2
  Enabled Cipher Suites:
    RSA_WITH_RC4_128_MD5,
    RSA_WITH_3DES_EDE_CBC_SHA,
    RSA_EXPORT_WITH_RC4_40_MD5
  Session Cache Timeout: 1200

Switch#
```

40.2. ssl-service-policy

Данная команда используется для настройки политики SSL Service Policy.

ssl-service-policy *POLICY-NAME* **[ciphersuite [rsa-null-md5] [rsa-null-sha][rsa-des-sha][rsa-3des-sha][dh-rsa-des-sha][dh-rsa-3des-sha][rsa-exp1024-des-sha][rsa-with-aes-128-cbc-sha][rsa-with-aes-256-cbc-sha][dhe-rsa-with-aes-128-cbc-sha][dhe-rsa-with-aes-256-cbc-sha] | session-cache-timeout** *TIME-OUT***]**

no ssl-service-policy *POLICY-NAME* **[{ciphersuite [rsa-null-md5] [rsa-null-sha][rsa-des-sha][rsa-3des-sha][dh-rsa-des-sha][dh-rsa-3des-sha][rsa-exp1024-des-sha][rsa-with-aes-128-cbc-sha][rsa-with-aes-256-cbc-sha][dhe-rsa-with-aes-128-cbc-sha][dhe-rsa-with-aes-256-cbc-sha]}|{session-cache-timeout}]**

Параметры

POLICY-NAME	Укажите имя политики SSL Service Policy.
ciphersuite	(Опционально) Укажите шифрование Cipher Suite, которое будет использовать служба безопасности при установлении соединения с удаленным узлом. Используйте обмен ключами RSA с шифрованием NULL и Message Digest 5 (MD5) для дайджеста сообщений – **rsa-null-md5**. Используйте обмен ключами RSA с шифрованием NULL и Secure Hash Algorithm (SHA) для дайджеста сообщений – **rsa-null-sha**. Используйте обмен ключами RSA с шифрованием DES и SHA для дайджеста сообщений – **rsa-des-sha**. Используйте обмен ключами RSA с шифрованием 3DES и SHA для дайджеста сообщений – **rsa-3des-sha**. Используйте обмен ключами DH и RSA с шифрованием DES и SHA для дайджеста сообщений – **dh-rsa-des-sha**. Используйте обмен ключами DH и RSA с шифрованием 3DES и SHA для дайджеста сообщений – **dh-rsa-3des-sha**. Используйте обмен ключами RSA с шифрованием EXP1024-DES и SHA для дайджеста сообщений – **rsa-exp1024-des-sha**. Используйте обмен ключами RSA с 128-битным шифрованием AES и CBC и SHA для дайджеста сообщений – **rsa-with-aes-128-cbc-sha**. Используйте обмен ключами RSA с 256-битным шифрованием AES и CBC и SHA для дайджеста сообщений – **rsa-with-aes-256-cbc-sha**. Используйте обмен ключами DH и RSA с 128-битным шифрованием AES и CBC и SHA для дайджеста сообщений – **dhe-rsa-with-aes-128-cbc-sha**.

	Используйте обмен ключами DH и RSA с 256-битным шифрованием AES и CBC и SHA для дайджеста сообщений – **dhe-rsa-with-aes-256-cbc-sha**.
session-cache-timeout *TIME-OUT*	(Опционально) Укажите значение тайм-аута в секундах для информации, хранящейся в кэше SSL-сессий. Доступный диапазон значений: от 60 до 86400. Если данный параметр не настроен, тайм-аут кэша сессий по умолчанию составляет 600 секунд. Используйте форму **no**, чтобы вернуть настройки по умолчанию для тайм-аута кэша SSL-сессий.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы настроить политику SSL Service Policy.

Пример

В данном примере показано, как настроить политику SSL Service Policy, которая ассоциирована с Trust Point «TP1». Настроенная политика SSL Service Policy – «ssl-server».

```
Switch# configure terminal
Switch(config)# ssl-service-policy ssl-server ciphersuite rsa-null-md5
Switch(config)#
```

40.3. show ssl-global-setting

Данная команда используется для отображения глобальных настроек SSL.

show ssl-global-setting

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить состояние SSL.

Пример

В данном примере показано, как отобразить глобальные настройки SSL.

```
Switch# show ssl-global-setting

ssl server state: Disable
ssl service policy name:
Switch#
```

41. Команды протокола Simple Network Management Protocol (SNMP)

41.1. 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

Любой режим конфигурирования

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
Trap Source Interface          : vlan1

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#
```

41.2. snmp-server

Данная команда используется для включения агента SNMP. Для выключения агента SNMP воспользуйтесь формой **no**.

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)#
```

41.3. snmp-server contact

Данная команда используется для настройки системной контактной информации для устройства. Для удаления настроек воспользуйтесь формой **no**.

snmp-server contact *TEXT*

no snmp-server contact

Параметры

contact *TEXT*	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)#
```

41.4. snmp-server enable traps

Данная команда используется для глобального включения отправки SNMP trap. Для отключения отправки SNMP trap воспользуйтесь формой **no**.

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)#
```

41.5. snmp-server enable traps snmp

Данная команда используется для включения отправки всех или определенных SNMP-уведомлений. Для отключения отправки всех или определенных SNMP-уведомлений воспользуйтесь формой **no**.

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)#
```

41.6. snmp-server location

Данная команда используется для указания информации о системном местоположении. Для удаления настроек воспользуйтесь формой **no**.

snmp-server location *TEXT*

no snmp-server location

Параметры

location *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)#
```

41.7. snmp-server name

Данная команда используется для указания информации о системном имени. Для удаления настроек воспользуйтесь формой **no**.

snmp-server name *NAME*

no snmp-server name

Параметры

NAME	Укажите имя SNMP-сервера. Максимально допустимое количество символов в строке – 64. Имя должно начинаться с буквы и заканчиваться буквой или цифрой. Дефисы между начальными и конечными символами

	допустимы. 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
SiteA-switch(config)#
```

41.8. snmp-server service-port

Данная команда используется для настройки номера UDP-порта SNMP. Для сброса номера UDP-порта к значениям по умолчанию воспользуйтесь формой **no**.

snmp-server service-port *PORT-NUMBER*

no snmp-server service-port

Параметры

PORT-NUMBER	Укажите номер UDP-порта. Доступный диапазон значений: от 1 до 65535. Некоторые номера могут конфликтовать с другими протоколами.

По умолчанию

Номер по умолчанию – 161.

Режим ввода команды

Global Configuration Mode

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)#
```

41.9. snmp-server response broadcast-request

Данная команда используется для включения разрешения серверу отвечать на широковещательные пакеты SNMP GetRequest. Для того чтобы запретить серверу отвечать на широковещательные пакеты SNMP GetRequest воспользуйтесь формой **no**.

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)#
```

41.10. 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

Любой режим конфигурирования

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: 000000090200000000C025808

Switch#
```

41.11. 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

Любой режим конфигурирования

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#
```

41.12. snmp-server community

Данная команда используется для настройки строки идентификатора сообщества (Community String) для доступа к SNMP. Для удаления строки Community String воспользуйтесь формой **no**.

snmp-server community [0 | 7] *COMMUNITY-STRING* **[view** *VIEW-NAME***] [ro | rw] [access** *IP-ACL-NAME***]**

no snmp-server community *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	Установите список управления доступом (ACL) для сообщества.
IP-ACL-NAME	(Опционально) Укажите имя стандартного списка

	доступа, дающего возможность пользователю использовать указанную строку Community String при доступе к агенту SNMP. Укажите доступного пользователя в поле адреса источника записи списка доступа.

По умолчанию

Community	View Name	Access right
private	CommunityView	Read/Write (чтение/запись)
public	CommunityView	Read Only (только чтение)

Режим ввода команды

Global Configuration Mode

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)#
```

41.13. snmp-server engineID local

Данная команда используется для указания SNMP engine ID на локальном устройстве. Для возврата SNMP engine ID к настройкам по умолчанию воспользуйтесь формой **no**.

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

Нет.

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)#
```

41.14. snmp-server group

Данная команда используется для настройки SNMP-группы. Для удаления SNMP-группы или удаления группы из используемой указанной модели безопасности воспользуйтесь формой **no**.

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 для аутентификации пакетов. Данный параметр не используется для шифрования пакетов.
noauth	Укажите для отмены аутентификации и шифрования пакетов.
priv	Укажите для аутентификации и шифрования пакетов.
read *READ-VIEW*	(Опционально) Укажите, чтобы обеспечить доступ 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 Name
Initial	SNMPv3	noauth	Restricted	None	Restricted
ReadGroup	SNMPv1	noauth	CommunityView	None	CommunityView
ReadGroup	SNMPv2c	noauth	CommunityView	None	CommunityView
WriteGroup	SNMPv1	noauth	CommunityView	CommunityView	CommunityView
WriteGroup	SNMPv2c	noauth	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)#
```

41.15. snmp-server host

Данная команда используется для указания получателя SNMP-уведомлений. Для удаления получателя воспользуйтесь формой **no**.

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	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-NUMBER	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)#
```

41.16. 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. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

41.17. snmp-server user

Данная команда используется для создания SNMP-пользователя. Для удаления SNMP-пользователя воспользуйтесь формой **no**.

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.
v3	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv3.
encrypted	(Опционально) Укажите для шифрования пароля.
auth	(Опционально) Укажите тип аутентификации.
md5	Укажите использование аутентификации MAC-MD5-96.
sha	Укажите использование аутентификации HMAC-SHA-96.

AUTH-PASSWORD	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-PASSWORD	Укажите ключ конфиденциальности, используемый алгоритмом DES. В форме обычного текста пароль может содержать от 8 до 16 символов. При указании параметра **encrypted** фиксированная длина пароля составляет 32 символа.
access *IP-ACL-NAME*	(Опционально) Укажите стандартный IP-адрес ACL для ассоциирования с пользователем.

По умолчанию

По умолчанию настроен один пользователь.

Имя пользователя – initial.

Имя группы – initial.

Режим ввода команды

Global Configuration Mode

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)#
```

41.18. snmp-server view

Данная команда используется для создания или изменения записи View. Для удаления указанной записи SNMP View воспользуйтесь формой **no**.

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, 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)#
```

42. Команды Spanning Tree Protocol (STP)

42.1. clear spanning-tree detected-protocols

Данная команда используется для перезапуска процесса миграции протокола.

clear spanning-tree detected-protocols {all | interface *INTERFACE-ID* **| port-channel** *<1-8>***}**

Параметры

all	Укажите, чтобы запустить действие обнаружения для всех портов.
interface *INTERFACE-ID*	Укажите интерфейс порта, на котором необходимо запустить действие обнаружения.
port-channel *<1-8>*	Укажите агрегированную группу (Channel Group), чтобы 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#
```

42.2. 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>* **[, | -] | port-channel** *<1-8>***} | mpt** *INSTANCE-ID* **]**

Параметры

interface *INTERFACE-ID*	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.
port-channel *<1-8>*	Укажите агрегированную группу (Channel Group), чтобы отобразить информацию.
mpt *INSTANCE-ID*	Укажите экземпляр Multi-process RSTP для отображения информации.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

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

Global Spanning Tree Status:
  Spanning Tree: Enabled
  STP New Root Trap: Disabled
  STP Topology Change Trap: Disabled
  Protocol Mode: RSTP
  Priority: 32768
  Bridge Max Age: 20
  Bridge Hello Time: 2
  Bridge Forward Time: 15
  TX Hold Count: 6
  Max Hops: 20
  Topology Change 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#
```

42.3. show spanning-tree configuration interface

Данная команда используется для отображения информации о настройках интерфейса STP.

show spanning-tree configuration interface [{*INTERFACE-ID* **[, | -] | port-channel** *<1-8>***}]**

Параметры

interface *INTERFACE-ID*	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.
port-channel *<1-8>*	Укажите агрегированную группу (Channel Group), чтобы отобразить информацию.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

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: auto
 Guard root: Disabled
 TCN filter : Disabled
 Bpdu forward: Disabled
 Hello Time  : 2

Switch#
```

42.4. snmp-server enable traps stp

Данная команда используется для включения отправки SNMP-уведомлений для STP. Для отключения отправки уведомлений для STP воспользуйтесь формой **no**.

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 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)#
```

42.5. spanning-tree global state

Данная команда используется для включения/отключения глобального состояния STP. Для отключения глобального состояния STP воспользуйтесь формой **no**.

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)#
```

42.6. spanning-tree (timers)

Данная команда используется для настройки значений таймеров Spanning Tree. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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 назначенного порта 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)#
```

42.7. spanning-tree state

Данная команда используется для включения/отключения STP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

spanning-tree state {enable | disable}

no spanning-tree state

Параметры

enable	Укажите, чтобы включить STP для сконфигурированного интерфейса.
disable	Укажите, чтобы отключить STP для сконфигурированного интерфейса.

По умолчанию

По умолчанию 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)#
```

42.8. spanning-tree cost

Данная команда используется для настройки значения стоимости пути на указанном порту. Для определения стоимости пути автоматически воспользуйтесь формой **no**.

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)#
```

42.9. spanning-tree guard root

Данная команда используется для включения функции STP Root Guard. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

42.10. spanning-tree link-type

Данная команда используется для настройки типа соединения (Link-type) для порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

42.11. spanning-tree mode

Данная команда используется для настройки режима STP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

42.12. spanning-tree portfast

Данная команда используется для настройки режима Port Fast на порту. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

42.13. spanning-tree port-priority

Данная команда используется для настройки значения приоритета STP на указанном порту. Команда применима только для версий RSTP и STP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

42.14. spanning-tree priority

Данная команда используется для настройки приоритета моста. Команда применима только для версий RSTP и STP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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 значения 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)#
```

42.15. spanning-tree tcnfilter

Данная команда используется для включения фильтрации уведомлений об изменении топологии сети TCN (Topology Change Notification) на указанном интерфейсе. Для отключения фильтрации TCN воспользуйтесь формой **no**.

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)#
```

42.16. spanning-tree tx-hold-count

Данная команда используется для ограничения максимального количества BPDU, которые могут быть отправлены перед паузой в одну секунду. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

42.17. spanning-tree forward-bpdu

Данная команда используется для включения BDPU Forwarding в Spanning Tree. Для отключения BDPU Forwarding в Spanning Tree воспользуйтесь формой **no**.

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 1/0/1
Switch(config-if)# spanning-tree forward-bpdu
Switch(config-if)#
```

43. Команды Storm Control

43.1. snmp-server enable traps storm-control

Данная команда используется для включения и настройки отправки SNMP-уведомлений для Storm Control. Для отключения отправки SNMP-уведомлений воспользуйтесь формой **no**.

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

Команды с ключевыми словами **storm-occur** и **storm-clear** включает или отключает уведомления для модуля Storm Control. Если дополнительные ключевые слова не указаны, уведомления **storm-occur** и **storm-clear** будут включены или отключены. При вводе команды с ключевым словом, включается или отключается только указанный тип уведомления.

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)#
```

43.2. storm-control

Данная команда используется для защиты устройства от штормовых атак широковещательных и многоадресных пакетов или пакетов с неизвестным адресом назначения. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

storm-control {{broadcast | multicast | unicast} level {pps *PPS-RISE* **[***PPS-LOW***] | kbps** *KBPS-RISE* **[***KBPS-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 0 до 2147483647. Если минимальный уровень (Low Level) PPS не указан, значение по умолчанию составляет 80% от указанного максимального (Rise) PPS.
level kbps *KBPS-RISE* **[***KBPS-LOW***]**	Укажите пороговое значение скорости передачи трафика, полученного на порту, в битах в секунду. Доступный диапазон значений: от 0 до 2147483647. Если минимальный уровень (Low Level) KBPS не указан, значение по умолчанию составляет 80% от указанного максимального (Rise) KBPS.
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.

Восстановить порт при возникновении ошибки можно двумя способами.

Пользователь может использовать команду **errdisable recovery cause**, чтобы включить автоматическое восстановление портов, которые были отключены по ошибке Storm Control.

Пользователь может вручную восстановить порт, введя команду **shutdown**, а затем команду **no shutdown** для порта.

Существует только один режим (в процентах, кбит/с или PPS), который может быть применен на интерфейсе. На интерфейсе, если указанный позже параметр режима отличается от предыдущего режима, предыдущие настроенные штормы будут сброшены до состояния по умолчанию (отключены в этой спецификации).

Из-за аппаратных ограничений, когда режим установлен в процентах или кбит/с:

- Действие не может быть задано для режима Shutdown (отключение).
- Для режимов Drop (отбрасывание), None (без действия) отсутствуют трапы и журналы.

Эта функция не может дать точный уровень подавления общей полосы пропускания в процентах (от 0 до 100) для определенного физического интерфейса. Текущая формула расчета предполагает, что размер пакета составляет 64 байта.

Пример

В данном примере показано, как включить Storm Control для управления широковещательным штормом на интерфейсе Ethernet 1/0/1. На Ethernet 3/0/1 установлен порог до 500 пакетов в секунду с действием отключения (Shutdown).

```
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
```

43.3. storm-control polling

Данная команда используется для настройки интервала опроса (Polling Interval) для подсчета количества полученных пакетов. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

43.4. show storm-control

Данная команда используется для отображения текущих настроек функции Storm Control.

show storm-control interface *INTERFACE-ID* **[, | -] [broadcast | multicast | unicast]**

Параметры

INTERFACE-ID	Укажите ID интерфейса порта.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
broadcast	Укажите, чтобы отобразить текущие настройки шторма широковещательных пакетов (Broadcast Storm).
multicast	Укажите, чтобы отобразить текущие настройки шторма многоадресных пакетов (Multicast Storm).
unicast	Укажите, чтобы отобразить текущие настройки шторма одноадресных пакетов (DLF).

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

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 range ethernet 1/0/1-1/0/6 broadcast

Polling Interval       : 15 sec           Shutdown Retries       : Infinite
Trap                   : Disabled
Interface    Storm      Action    Threshold         Current    State
-------------------------------------------------------------
eth1/0/1     Broadcast  Drop      500/300 pps       200 pps    Forwarding
eth1/0/2     Broadcast  Drop      80/64 %           20 %       Forwarding
eth1/0/3     Broadcast  Drop      80/64 %           70 %       Dropped
eth1/0/4     Broadcast  Shutdown  60/50 %           20 %       Forwarding
eth1/0/5     Broadcast  None      60000/50000 kbps  2000 kbps  Forwarding
eth1/0/6     Broadcast  None      -                 -          Inactive

Total Entries: 6

Switch#
```

В данном примере показано, как отобразить все настройки для диапазона интерфейсов от 1/0/1 до 1/0/2.

```
Switch# show storm-control interface ethernet 1/0/1-2

Polling Interval       : 15 sec           Shutdown Retries       : Infinite
Trap                      : Disabled
Interface      Storm         Action      Threshold     Current    State
---------------------- -------------------------------------------
ethernet 1/0/1      Broadcast     Drop         80/64 %       50%        Forwarding
ethernet 1/0/1      Multicast     Drop         80/64 %       50%        Forwarding
ethernet 1/0/1      Unicast       Drop         80/64 %       50%        Forwarding
ethernet 1/0/2      Broadcast    Shutdown     500/300 pps   -          Error
Disabled
ethernet 1/0/2      Multicast    Shutdown     500/300 pps   -          Error
Disabled
ethernet 1/0/2      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.

43.5. show snmp-server traps storm-control

Данная команда используется для отображения состояния отправки уведомлений для функции Storm Control.

show snmp-server traps storm-control

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить состояние оправки уведомлений для функции Storm Control.

Пример

В данном примере показано, как отобразить состояние оправки уведомлений для функции Storm Control.

```
Switch# show snmp-server traps storm-control
  storm occur                : Disabled
  storm clear                : Disabled
Switch#
```

44. Команды Surveillance VLAN

44.1. surveillance vlan

Данная команда используется для глобального включения функции Surveillance VLAN и ее настройки. Для отключения функции Surveillance VLAN воспользуйтесь формой **no**.

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)#
```

44.2. surveillance vlan aging

Данная команда используется для настройки времени устаревания (Aging Time) для устаревших динамических Member-портов Surveillance VLAN. Для сброса времени устаревания до настроек по умолчанию воспользуйтесь формой **no**.

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)#
```

44.3. surveillance vlan enable

Данная команда используется для включения функции Surveillance VLAN на портах. Для отключения функции Surveillance VLAN на портах воспользуйтесь формой **no**.

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.

Используйте данную команду, чтобы включить функцию Surveillance VLAN на 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)#
```

44.4. surveillance vlan mac-address

Данная команда используется для добавления определенного пользователем OUI (уникального идентификатора организации) устройства Surveillance. Для удаления определенного пользователем OUI устройства Surveillance воспользуйтесь формой **no**.

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 компоненты Surveillance, которые могут быть автоматически обнаружены при помощи Surveillance VLAN.
vms	(Опционально) Укажите, чтобы выбрать VMS (Video Management Server – сервер для управления системой видеонаблюдения) в качестве типа компонентов Surveillance.
vms-client	(Опционально) Укажите клиента VMS в качестве типа компонентов Surveillance.
video-encoder	(Опционально) Укажите видеокодер в качестве типа компонентов Surveillance.
network-storage	(Опционально) Укажите сетевое хранилище в качестве типа компонентов Surveillance.
other	(Опционально) Укажите другое сетевое устройство для наблюдения в качестве типа компонентов Surveillance.
description *TEXT*	(Опционально) Укажите описание определенного пользователем OUI. Максимально допустимое количество символов – 32.

По умолчанию

Адрес OUI	Маска	Тип компонента	Описание
28-10-7B-00-00-00	FF-FF-FF-E0-00-00	Устройство D-Link	Сетевое устройство для наблюдения
28-10-7B-20-00-00	FF-FF-FF-F0-00-00	Устройство D-Link	Сетевое устройство для наблюдения

B0-C5-54-00-00-00	FF-FF-FF-80-00-00	Устройство D-Link	Сетевое устройство для наблюдения
F0-7D-68-00-00-00	FF-FF-FF-F0-00-00	Устройство D-Link	Сетевое устройство для наблюдения

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для добавления одного или нескольких определенных пользователем OUI Surveillance VLAN. OUI используется для идентификации трафика Surveillance с помощью функции Surveillance VLAN.

Если MAC-адреса источника полученных пакетов соответствуют любому из шаблонов OUI, полученный пакет распознается как surveillance.

Определенный пользователем OUI не может совпадать с OUI по умолчанию.

OUI по умолчанию не может быть удален.

Пример

В данном примере показано, как добавить определенный пользователем OUI для 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)#
```

44.5. surveillance vlan qos

Данная команда используется для настройки приоритета CoS для входящего трафика Surveillance VLAN. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

surveillance vlan qos *COS-VALUE*

no surveillance vlan qos

Параметры

COS-VALUE	Укажите приоритет Surveillance VLAN в диапазоне от 0 до 7.

По умолчанию

Значение по умолчанию – 5.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для маркировки CoS пакетов Surveillance, поступающих на порт, на котором включена Surveillance VLAN. Маркировка CoS позволяет отделить трафик Surveillance VLAN от трафика данных по качеству обслуживания.

Пример

В данном примере показано, как настроить приоритет Surveillance VLAN со значением 7.

```
Switch# configure terminal
Switch(config)# surveillance vlan qos 7
Switch(config)#
```

44.6. show surveillance vlan

Данная команда используется для отображения настроек Surveillance VLAN.

show surveillance vlan [interface [*INTERFACE-ID* **[, | -]]]**

show surveillance vlan device [interface [*INTERFACE-ID* **[, | -]]]**

Параметры

device	Укажите, чтобы отобразить информацию об изученных устройствах Surveillance.
interface	(Опционально) Укажите, чтобы отобразить информацию о Surveillance VLAN на портах.
INTERFACE-ID	(Опционально) Укажите порт, о котором необходимо отобразить информацию.
,	(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

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения настроек Surveillance VLAN.

Для отображения глобальных настроек Surveillance VLAN используйте команду **show surveillance vlan**.

Для отображения настроек Surveillance VLAN на интерфейсах используйте команду **show surveillance vlan interface**.

Для отображения устройства Surveillance, информация о котором была получена через OUI, используйте команду **show surveillance vlan device**.

Пример

В данном примере показано, как отобразить глобальные настройки Surveillance VLAN.

```
Switch# show surveillance vlan

 Surveillance VLAN State : Enabled
 Surveillance VLAN ID  : 100
 Surveillance VLAN CoS : 5
 Aging Time            : 30 minutes

 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#
```

45. Команды Secure Shell (SSH)

45.1. 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# show ssh
No SSH connections running.
Switch# crypto key generate rsa
Choose the size of the key modulus in the range of 1024 or 2048. The process may
take a few minutes.
Number of bits in the modulus [1024]:

Generating RSA key...Done.


Switch#
```

45.2. 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

Данная команда используется для удаления пары ключей RSA или DSA.

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#
```

45.3. ip ssh timeout

Данная команда используется для настройки параметров контроля SSH на коммутаторе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

ip ssh {timeout *SECONDS* **| authentication-retries** *NUMBER***}**

no ip ssh {timeout | authentication-retries}

Параметры

timeout *SECONDS*	Укажите временной интервал ожидания ответа от SSH-клиента для этапа согласования SSH. Диапазон значений: от 30 до 600.
authentication-retries *NUMBER*	Укажите количество попыток аутентификации. Сессия завершается после всех неудачных попыток. 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 180 секунд.

```
Switch# configure terminal
Switch(config)# ip ssh timeout 180
Switch(config)#
```

45.4. ip ssh server

Данная команда используется для включения SSH-сервера. Для отключения SSH-сервера воспользуйтесь формой **no**.

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)#
```

45.5. ip ssh service-port

Данная команда используется для указания сервисного порта для SSH. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

ip ssh service-port *TCP-PORT*

no ip ssh service-port

Параметры

TCP-PORT	Укажите номер TCP-порта. Диапазон значений: от 1 до 65535. Как правило, для протокола SSH назначается TCP-порт 22.

По умолчанию

По умолчанию номер TCP-порта – 22.

Режим ввода команды

Global Configuration Mode

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 – 2400.

```
Switch# configure terminal
Switch(config)# ip ssh service-port 2400
Switch(config)#
```

45.6. 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

Любой режим конфигурирования

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: 01:20:11,2021-01-01
Key Size: 1024 bits
Key Data:
AAAAB3Nz aC1yc2EA AAADAQAB AAAAgQC4 zriByG80 ik+rp2Bj vPmQiosQ e1vRt08c
yarhE4A1 EafTsg+R qH90mxZH F1bmfcqd lTnFXV1m PRfgWt4M Q/SySe1N 7ScDcsFZ
SNLLyOaU sRLonwvC fq8VQVYy UD0PoolO huHkLrc9 wpZjjmNL o/kTbpzF xj9N+miz
c47A+IPG Pw==
Switch#
```

45.7. 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

Любой режим конфигурирования

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 текущей сессии SSH.

```
Switch# show ssh

SID   Ver.  Cipher                        Userid     Client IP Address
---   ----  ------------------------      ---------  -----------------
0     V2    aes256-ctr/hmac-sha1          test       192.168.0.113

Total Entries: 1
```

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.

45.8. show ip ssh

Данная команда используется для отображения конфигурации SSH-сервера.

show ip ssh

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить состояние SSH-сервера на коммутаторе.

Пример

В данном примере показано, как отобразить состояние SSH-сервера.

```
Switch# show ip ssh
IP SSH server                  :Enabled
IP SSH service port            :22
SSH server mode                :V2
Authentication timeout         :180   secs
Authentication retries         :3     times
Switch#
```

45.9. ssh user authentication-method

Данная команда используется для настройки методов аутентификации SSH для учетной записи пользователя. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

ssh user *USERNAME* **authentication-method {password | publickey | hostbased host-name** *HOSTNAME* **[***IP-ADDRESS* **|** *IPV6-ADDRESS***]}**

no ssh user *USERNAME* **authentication-method**

Параметры

USERNAME	Укажите имя пользователя для настройки типа аутентификации. Имя пользователя должно быть существующей локальной учетной записью. Максимальное количество символов – 32.
password	Укажите метод аутентификации по паролю для указанной учетной записи пользователя. Данный метод аутентификации используется по умолчанию.
publickey	Укажите метод аутентификации с открытым ключом для указанной учетной записи пользователя.
hostbased host-name *HOSTNAME*	Укажите доступное имя узла для аутентификации на основе узла. Имя узла клиента проверяется во время аутентификации. Диапазон значений: от 1 до 255.
IP-ADDRESS	(Опционально) Укажите необходима ли дополнительная проверка IP-адреса клиента для аутентификации на основе узла. Если не указано, будет проверено только

	имя узла.
IPV6-ADDRESS	(Опционально) Укажите необходима ли дополнительная проверка IPv6-адреса клиента для аутентификации на основе узла. Если не указано, будет проверено только имя узла.

По умолчанию

По умолчанию используется метод аутентификации по паролю.

Режим ввода команды

Global Configuration Mode

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.

Пример

В данном примере показано, как создать пользователя «test» и настроить для него метод аутентификации SSH по паролю.

```
Switch(config)# username test privilege 15 password 1234
Switch(config)# ssh user test authentication-method password
Switch(config)#
```

46. Команды портов коммутатора

46.1. duplex

Данная команда используется для настройки режима дуплекса на интерфейсе физического порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

duplex {full | auto}

no duplex

Параметры

full	Укажите для работы порта в режиме полного дуплекса (Full-Duplex Mode).
auto	Укажите, чтобы режим дуплекса на порту был определен автосогласованием (Auto-Negotiation).

По умолчанию

Для интерфейса 1000Base-T параметр по умолчанию – **auto**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12.

Использование команды

Чтобы включить функцию автосогласования, необходимо указать параметр **auto** или для скорости, или для режима дуплекса. При фиксированном значении режима дуплекса и указании параметра **auto** для скорости будет согласована только скорость. Может быть установлена любая скорость в зависимости от выбранного режима дуплекса. При фиксированном значении скорости и указании параметра **auto** для режима дуплекса будет согласован только режим дуплекса. Может быть установлен режим полного дуплекса или полудуплекса в зависимости от выбранной скорости.

Пример

В данном примере показано, как установить фиксированную скорость 100 Мбит/с и настроить режим дуплекса, определенный автосогласованием, на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)# speed 100
Switch(config-if)# duplex auto
Switch(config-if)#
```

46.2. flowcontrol

Данная команда используется для настройки возможности управления потоком (Flow Control) на интерфейсе порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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.

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)#
```

46.3. speed

Данная команда используется для настройки скорости интерфейса физического порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

speed { 100 | 1000 | 10giga | 2.5giga |5giga | auto }

no speed

Параметры

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).
10giga	Укажите, чтобы установить скорость 10 Гбит/с.
2.5giga	Укажите, чтобы установить скорость 2,5 Гбит/с.
5giga	Укажите, чтобы установить скорость 5 Гбит/с.
auto	Укажите, чтобы скорость и управление потоком медных портов с оборудованием на противоположной стороне были заданы при помощи автосогласования. Укажите, чтобы включить на оптических портах (1000Base-SX/LX) функцию автосогласования, с помощью которой время и управление потоком будут согласованы с оборудованием на противоположной стороне.

По умолчанию

Для интерфейса 1000Base-T по умолчанию скорость определяется автоматически.

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.

Если скорость установлена на 1000 Мбит/с или 10 Гбит/с, то дуплексный режим не может быть установлен на полудуплексный. Если для дуплексного режима установлено значение

полудуплексный, то скорость не может быть установлена на 1000 Мбит/с или 10 Гбит/с.

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. Может быть установлен режим полного дуплекса или полудуплекса в зависимости от выбранной скорости.

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 100,1000
Switch(config-if)#
```

47. Команды управления системных файлов

47.1. boot image

Данная команда используется для указания файла образа, который будет использован при следующем запуске устройства.

boot image *IMAGE-ID*

Параметры

IMAGE-ID	Укажите ID образа 1 или 2.

По умолчанию

По умолчанию используется загрузочный файл образа.

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 ID образа 1 в качестве файла образа для загрузки.

```
Switch# configure terminal
Switch(config)# boot imageid 1
Switch(config)#
```

47.2. 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

Privilege 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...
```

47.3. copy

Данная команда используется для копирования файлов.

copy imageid *IMAGE-ID tftp://LOCATION/DESTINATION-URL*

copy log *tftp://LOCATION/DESTINATION-URL*

copy running-config {startup-config| *tftp://LOCATION/DESTINATION-URL* **| config1| config2}**

copy startup-config *tftp://LOCATION/DESTINATION-URL*

copy *tftp://LOCATION/SOURCE-URL*

copy *tftp://LOCATION/SOURCE-URL* **startup-config**

Параметры

LOCATION	(Опционально) Укажите IPv4-адрес или IPv6-адрес TFTP-сервера.
imageid	Параметр imageid используется для резервного копирования.
IMAGE-ID	Укажите ID образа 1 или 2.
tftp://LOCATION/DESTINATION-URL	Имя файла с указанием пути к серверу tftp://location/filename. Команда copy tftp://LOCATION/SOURCE-URL используется для обновления файла образа.
log	Резервное копирование текущего файла журнала.
running-config	Резервное копирование текущей конфигурации системы.
startup-config	Резервное копирование загрузочной конфигурации.
config1	Сохранить на config1.
config2	Сохранить на config2.

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 startup-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 imageid**.

Пример

В данном примере показано, как выгрузить текущую конфигурацию или загрузочную конфигурацию на TFTP-сервер для хранения.

```
Switch# copy running-config tftp://10.1.1.254/cfg.bin
Address of remote host [10.1.1.254]?
Destination filename [cfg.bin]?
 Accessing tftp://10.1.1.254/cfg.bin...
 Transmission start...
 Transmission finished.
 Configuration backup successful.
Switch#

Switch# copy startup-config tftp://10.1.1.254/startupcfg.bin
 Accessing tftp://10.1.1.254/startupcfg.bin
 Transmission start...
 Transmission finished.
 Configuration backup successful.
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#

Switch# copy running-config config1
Destination filename startup-config? [y/n]: y

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

Switch# copy running-config config2
Destination filename startup-config? [y/n]: y
Saving all configurations to NV-RAM..... Done.
Switch#
```

В данном примере показано, как загрузить файл образа с TFTP-сервера на неактивный образ.

```
Switch# copy tftp://10.1.1.254/image2
TFTP Firmware Upgrade processing...................Do not power off!!
Firmware upgrade successfully!
Switch#
```

В данном примере показано, как выгрузить файл образа на TFTP-сервер.

```
Switch# copy imageid 2 tftp://10.1.1.254/image2
Transfering firmware...................   100%
Firmware Backup successfully!
Switch#
```

В данном примере показано, как выгрузить журнал на TFTP-сервер для хранения.

```
Switch# copy log tftp://10.1.1.254/log.txt
 Accessing tftp://10.1.1.254/log.txt
 Transmission start...
 Transmission finished.
 Syslog backup successful.
Switch#
```

47.4. show boot

Данная команда используется для отображения настроек загрузочного конфигурационного файла и загрузочного образа.

show boot

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 используется для отображения настроек конфигурационного файла и загрузочного образа.

Пример

В данном примере показано, как отобразить информацию о загрузке системы.

```
Switch# show boot

Boot image: image1
Boot config: config1
```

47.5. show running-config

Данная команда используется для отображения команд текущего конфигурационного файла.

show running-config

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда используется для отображения текущей конфигурации.

Пример

В данном примере показано, как отобразить содержимое текущего конфигурационного файла.

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

# Basic
# LACP
configure terminal
lacp system-priority 32768
port-channel load-balance src-mac
interface range ethernet 1/0/1-2
channel-group 1 mode on
exit
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
CTRL+C ESC q Quit SPACE n Next PageENTER Next Entry a All
```

47.6. show startup-config

Данная команда используется для отображения содержимого загрузочного конфигурационного файла.

show startup-config

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда используется для отображения настроек конфигурации, с помощью которых система будет инициализирована.

Пример

В данном примере показано, как отобразить содержимое загрузочного конфигурационного файла.

```
Switch# show startup-config
#------------------------------------------------------------------------
#            DXS-1210-12SC 10GbE Smart Managed Switch Configuration
#
#                           Firmware: Build V1.15.003
#         Copyright(C) 2017 D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------
# Basic
# ------------------------------------------------------------
# LACP
configure terminal
lacp system-priority 32768
port-channel load-balance src-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
interface ethernet 1/0/4
lacp port-priority 32768
lacp timeout short
exit
interface ethernet 1/0/5
lacp port-priority 32768
lacp timeout short
exit
interface ethernet 1/0/6
CTRL+C ESC q Quit SPACE n Next PageENTER Next Entry a All
```

47.7. boot startup-config

Данная команда используется для установки загрузочного конфигурационного файла.

boot startup-config {config1 | config2}

Параметры

config1	Первая конфигурация.
config2	Вторая конфигурация.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда используется для установки загрузочного конфигурационного файла.

Пример

В данном примере показано, как установить загрузочного конфигурационного файла.

```
Switch(config)# boot startup-config config1
Switch(config)#
```

47.8. reboot

Данная команда используется для перезагрузки системы.

reboot [force_agree]

Параметры

force_agree	Принудительная перезагрузка без подтверждения пользователем.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда используется для перезагрузки системы.

Пример

В данном примере показано, как перезагрузить систему без подтверждения пользователем.

```
Switch# reboot force_agree
Switch#
```

48. Команды System Log

48.1. clear logging

Данная команда используется для удаления сообщений логирования из буфера системного логирования.

clear logging

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privilege 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#
```

48.2. logging buffered

Данная команда используется для включения логирования системных сообщений в локальный буфер сообщений. Для отключения логирования системных сообщений в локальный буфер сообщений воспользуйтесь формой **no**. Используйте команду **default logging buffered**, чтобы вернуть настройки по умолчанию.

logging buffered [severity {*SEVERITY-LEVEL* **|** *SEVERITY-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. Если значение не указано, значение уровня по умолчанию – warnings (4).
SEVERITY-NAME	(Опционально) Укажите название уровня важности системных сообщений. Имена уровней важности: emergencies, alerts, critical, errors, warnings, notifications, informational, debugging.
write-delay *SECONDS*	(Опционально) Укажите задержку периодической записи буфера логирования во FLASH-память на указанное количество секунд.
infinite	(Опционально) Укажите значение **infinite**, чтобы отключить периодическую запись буфера логирования на FLASH .

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 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)#
```

48.3. logging server

Данная команда используется для создания серверного узла SYSLOG для логирования системных сообщений или вывода при отладке. Для удаления серверного узла SYSLOG воспользуйтесь формой **no**.

logging server {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [severity {***SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [facility** *FACILITY-TYPE***] [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 будут логироваться на сервер логирования. Значение может быть от 0 до 7, где 0 – наиболее важный уровень. Если значение не указано, значение уровня по умолчанию – warnings (4).
SEVERITY-NAME	(Опционально) Укажите название уровня важности системных сообщений. Имена уровней важности: emergencies, alerts, critical, errors, warnings, notifications, informational, debugging.
FACILITY-TYPE	(Опционально) Укажите тип для facility в виде десятичного значения от 0 до 23. Если значение не указано, по умолчанию будут использоваться сообщения ядра (0).
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.

Числовой код	Facility
0	Сообщения ядра
1	Сообщения уровня пользователя
2	Система почты
3	Системные daemon
4	Сообщения системы безопасности/авторизации
5	Сообщения, генерируемые SYSLOG
6	Подсистема Line Printer
7	Подсистема сетевых новостей
8	Подсистема UUCP
9	Clock daemon
10	Сообщения системы безопасности/авторизации
11	FTP daemon
12	Подсистема NTP
13	Аудит логирования
14	Предупреждение логирования
15	Clock daemon (note 2)
16	Локальное использование 0 (local0)
17	Локальное использование 1 (local1)
18	Локальное использование 2 (local2)
19	Локальное использование 3 (local3)

20	Локальное использование 4 (local4)
21	Локальное использование 5 (local5)
22	Локальное использование 6 (local6)
23	Локальное использование 7 (local7)

Пример

В данном примере показано, как включить логирование системных сообщений с уровнем важности выше warnings на удаленном узле 20.3.3.3.

```
Switch# configure terminal
Switch(config)#logging server  20.3.3.3 severity warnings
Switch(config)#
```

48.4. logging source-interface

Данная команда используется для указания IP-адреса интерфейса, который будет использоваться в качестве адреса источника для отправки пакетов SYSLOG. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

48.5. show logging

Данная команда используется для просмотра системных сообщений, логированных в локальном буфере.

show logging [all | [*REF-SEQ***] [increase** *NN* **| decrease** *NN***]]**

show logging info

Параметры

all	Укажите для отображения всех записей лога, начиная с последних.
REF-SEQ	Укажите для отображения с номера, следующего за указанным.
increase *NN*	Укажите количество сообщений, появившихся после указанного номера, следующим за указанным. Если значение не указано, отображение начинается от самых давних сообщений в буфере.
decrease *NN*	Укажите количество сообщений, появившихся до указанного номера, следующим за указанным. Если значение не указано, отображение начинается от самых последних сообщений в буфере.
info	Укажите, чтобы отобразить глобальные настройки системного журнала.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

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 logging

Total number of buffered messages: 2

#2 2013-08-02 16:37:36 INFO(6) Logout through Console (Username: Anonymous)
#1 2013-08-02 16:35:54 INFO(6) Port ethernet 1/0/1 link up, 1000Mbps FULL duplex

switch#
```

48.6. command logging

Данная команда используется для включения функции логирования выполненных команд. Для отключения функции логирования воспользуйтесь формой **no**.

command logging enable

no command logging enable

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 1.

Использование команды

Команда логирования используется для записи выполненных команд.

Пример

В данном примере показано, как включить функцию логирования.

```
Switch(config)# command logging enable
```

49. Команды времени и SNTP

49.1. 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

Privilege 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 данном примере показано, как вручную установить системное время на 18:00, 4 июля 2014 г.

```
Switch# clock set 18:00:00 4 Jul 2014
Switch#
```

49.2. clock summer-time

Данная команда используется для настройки автоматического перехода на летнее время. Для отключения автоматического перехода на летнее время воспользуйтесь формой **no**.

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 месяц (от 1 до 12).
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 данном примере показано, как назначить начало летнего времени на 2 часа ночи первого воскресенья июня и конец на 2 часа ночи последнего воскресенья октября.

```
Switch# configure terminal
Switch(config)#clock summer-time recurring 1 sun jun 02:00 last sun oct 02:00
Switch(config)#
```

49.3. clock timezone

Данная команда используется для настройки и отображения часового пояса. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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 настройки 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)#
```

49.4. 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

Любой режим конфигурирования

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  : SNTP
Current Time         : 18:20:04, 2014-07-04
Time Zone            : UTC +02:30
Daylight Saving Time : Recurring
Offset in Minutes    : 30
    Recurring From   : Apr 2nd Tue 15:00
              To     : Oct 2nd Wed 15:30

Switch#
```

49.5. 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

Любой режим конфигурирования

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 Pool Interval  : 720 seconds

SNTP Server Status:

SNTP Server                                    Stratum Version Last Receive
---------------------------------------------- ------- ------- ---------------
10.0.0.11                                      8       4       00:02:02
10.0.0.12                              7       4       00:01:02 Synced
10::2                                          ------- ------- ---------------
FE80::1111vlan1                                ------- ------- ---------------
---------------------------------------------- ------- ------- ---------------

Total Entries:4

Switch#
```

49.6. sntp server

Данная команда используется для синхронизации системного времени с сервером SNTP. Для удаления сервера из списка серверов SNTP воспользуйтесь формой **no**.

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 отличие от NTP, не обеспечивает сложных механизмов фильтрации и статистической обработки. Кроме того, SNTP не проверяет подлинность трафика, хотя с

помощью настройки расширенного списка доступа можно обеспечить определённую степень защиты.

Чтобы создать несколько серверов SNTP, введите данную команду несколько раз, используя разные IP-адреса серверов SNTP.

Используйте форму **no**, чтобы удалить запись сервера SNTP. При удалении записи укажите точную информацию, введенную при первом подключении. Время, полученное с сервера SNTP, синхронизируется с форматом UTC.

Пример

В данном примере показано, как синхронизировать системное время с сервером SNTP с IP-адресом 192.168.22.44.

```
Switch# configure terminal
Switch(config)# sntp server 192.168.22.44
Switch(config)#
```

49.7. sntp enable

Данная команда используется для включения функции SNTP. Для отключения функции SNTP воспользуйтесь формой **no**.

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)#
```

49.8. sntp interval

Данная команда используется для настройки интервала синхронизации часов SNTP-клиента с сервером. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

50. Команды временного диапазона

50.1. periodic

Данная команда используется в режиме Time-Range Configuration Mode для указания профиля диапазона времени. Для удаления указанного временного диапазона воспользуйтесь формой **no**.

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 *WEEK-DAY HH:MM* **to [***WEEK-DAY***]** *HH:MM*	Укажите день недели (monday, tuesday, wednesday, thursday, friday, saturday, sunday) и время в формате ЧЧ:ММ. Конечный день недели, совпадающий с начальным, можно не указывать.

По умолчанию

Нет.

Режим ввода команды

Time-range Configuration Mode

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)#
```

50.2. 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

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если имя не указано, 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#
```

50.3. time-range

Данная команда используется для входа в режим Time-Range Configuration Mode для указания профиля диапазона времени. Для удаления временного диапазона воспользуйтесь формой **no**.

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.

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)#
```

51. Команды Traffic Segmentation

51.1. 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 ID интерфейса. 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

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

При вводе данной команды без каких-либо ключевых слов, отображается конфигурация Traffic Segmentation для всех портов. В противном случае отображается конфигурация Traffic Segmentation только для указанного интерфейса.

Пример

В данном примере показано, как отобразить конфигурацию Traffic Segmentation для интерфейса Ethernet 1/0/1.

```
Switch# show traffic-segmentation forward interface ethernet 1/0/1

Interface        Forwarding Domain
------------ ------------------------------------------
ethernet 1/0/1        ethernet 1/0/1, ethernet 1/0/4-6

Total Entries: 1

Switch#
```

51.2. traffic-segmentation forward

Данная команда используется для ограничения продвижения пакетов в L2 домене, приходящих на настроенный порт. Для удаления ограничения продвижения пакетов в L2 домене воспользуйтесь формой **no**.

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 с помощью 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 1/0/1 до Ethernet-порта 1/0/6.

```
Switch# configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)# traffic-segmentation forward interface range ethernet 1/0/1-6
Switch(config-if)#
```

52. Команды Virtual LAN (VLAN)

52.1. acceptable-frame

Данная команда используется для настройки допустимых типов кадров на порту. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

52.2. ingress-checking

Данная команда используется для включения проверки входящих кадров, получаемых портом. Для отключения проверки воспользуйтесь формой **no**.

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)#
```

52.3. show vlan

Данная команда используется для отображения параметров для всех настроенных VLAN или одной VLAN на коммутаторе.

show vlan [*VLAN-ID* **[, | -] | interface [***INTERFACE-ID* **[, | -]]]**

Параметры

VLAN-ID	(Опционально) Список VLAN для отображения информации о портах-участниках. Если VLAN не указана, то отображаются все VLAN. Корректный диапазон: от 1 до 4094.
interface *INTERFACE-ID*	(Опционально) Порт для отображения настроек, касающихся VLAN.
,	(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

Любой режим конфигурирования

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
   Tagged Member Ports   :
   Untagged Member Ports : 1/0/1-1/0/28

 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 ethernet 1/0/1-1/0/4

 ethernet 1/0/1
   VLAN mode              : Hybrid
   Native VLAN            : 1
   Hybrid untagged VLAN   : 1
   Hybrid tagged VLAN     :
   Ingress checking       : Enabled
   Acceptable frame type  : Admit-All
   Dynamic tagged VLAN    :

 ethernet 1/0/2
   VLAN mode              : Hybrid
   Native VLAN            : 1
   Hybrid untagged VLAN   : 1
   Hybrid tagged VLAN     :
   Ingress checking       : Enabled
   Acceptable frame type  : Admit-All
   Dynamic tagged VLAN    :

 ethernet 1/0/3
   VLAN mode              : Hybrid
   Native VLAN            : 1
   Hybrid untagged VLAN   : 1
   Hybrid tagged VLAN     :
   Ingress checking       : Enabled
   Acceptable frame type  : Admit-All
   Dynamic tagged VLAN    :

 ethernet 1/0/4
   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#
```

52.4. switchport access vlan

Данная команда используется для указания access VLAN для интерфейса. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

switchport access vlan *VLAN-ID*

no switchport access vlan

Параметры

access vlan *VLAN-ID*	Укажите 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). 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 интерфейс 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)#
```

52.5. switchport hybrid allowed vlan

Данная команда используется для указания тегированных или нетегированных VLAN для гибридного порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

switchport hybrid allowed vlan {[add] {tagged | untagged} | remove} *VLAN-ID* **[, | -]**

no switchport hybrid allowed vlan

Параметры

add	Укажите порт, который будет добавлен в указанную(-ые) VLAN.
remove	Укажите порт, который будет удален из указанной(-ых) VLAN.
tagged	Указывает порт в качестве тегированного для указанной(-ых) VLAN.
untagged	Указывает порт в качестве нетегированного для 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) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию гибридный порт является нетегированным членом VLAN 1.

Режим ввода команды

Interface Configuration Mode

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 интерфейс 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)#
```

52.6. switchport hybrid native vlan

Данная команда используется для указания native VLAN ID гибридного порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

switchport hybrid native vlan *VLAN-ID*

no switchport hybrid native vlan

Параметры

vlan *VLAN-ID*	Укажите 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 интерфейс 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)#
```

52.7. switchport mode

Данная команда используется для указания режима VLAN (VLAN mode) для порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

switchport mode {access | hybrid | trunk}

no switchport mode

Параметры

access	Укажите порт в качестве порта доступа.

hybrid	Укажите порт в качестве гибридного порта.
trunk	Укажите порт в качестве trunk-порта.

По умолчанию

По умолчанию установлена опция **hybrid**.

Режим ввода команды

Interface Configuration Mode

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.

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.

При изменении режима switch-port mode настройки, связанные с VLAN и ассоциированные с предыдущим режимом, будут утеряны.

Пример

В данном примере показано, как настроить интерфейс ethernet 1/0/1 в качестве trunk-порта.

```
Switch# configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)#
```

52.8. switchport trunk allowed vlan

Данная команда используется для настройки VLAN, которым разрешено получать и отправлять трафик на указанный интерфейс в тегированном формате. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

switchport trunk allowed vlan {all | [add | remove | except] *VLAN-ID* **[, | -]}**

no switchport trunk allowed vlan

Параметры

all	Укажите для разрешения всех VLAN 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) 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 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 интерфейс 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)#
```

52.9. switchport trunk native vlan

Данная команда используется для указания native VLAN ID интерфейса в режиме trunk mode. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

switchport trunk native vlan {*VLAN-ID* **| tag}**

no switchport trunk native vlan [tag]

Параметры

VLAN-ID	Укажите native VLAN для trunk-порта.
tag	Укажите, чтобы включить режим 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 интерфейс 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)#
```

52.10. vlan

Данная команда используется для добавления VLAN и входа в режим VLAN configuration

mode. Для удаления VLAN воспользуйтесь формой **no**.

vlan *VLAN-ID* **[, | -]**
no vlan *VLAN-ID* **[, | -]**

Параметры

VLAN-ID	Укажите идентификатор VLAN, который должен быть добавлен, удален или настроен. Корректный диапазон VLAN ID: от 1 до 4094. VLAN ID 1 не может быть удален.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

VLAN ID 1 существует в системе в качестве VLAN по умолчанию.

Режим ввода команды

Global Configuration Mode

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 до 1005.

```
Switch# configure terminal
Switch(config)#vlan 1000-1005
Switch(config-vlan)#
```

52.11. name

Данная команда используется для указания имени VLAN. Для сброса имени VLAN до имени VLAN по умолчанию воспользуйтесь формой **no**.

name *VLAN-NAME*

no name

Параметры

VLAN-NAME	Укажите имя VLAN. Максимально допустимое количество символов – 32. 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)#
```

53. Команды Voice VLAN

53.1. voice vlan

Данная команда используется для глобального включения функции Voice VLAN и её настройки. Для отключения функции Voice VLAN воспользуйтесь формой **no**.

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)#
```

53.2. voice vlan aging

Данная команда используется для настройки времени устаревания (Aging Time) для устаревших динамических Member-портов Voice VLAN. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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 голосового устройства и автоматически изученных Member-портов Voice VLAN. Когда последнее голосовое 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)#
```

53.3. voice vlan enable

Данная команда используется для включения функции Voice VLAN на портах. Для отключения функции Voice VLAN на портах воспользуйтесь формой **no**.

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

Используйте команду **voice vlan** в режиме Global Configuration Mode и **voice vlan enable** в режиме Interface Configuration Mode, чтобы включить функцию Voice VLAN на портах доступа или гибридных портах.

Пример

В данном примере показано, как включить функцию Voice VLAN на 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)#
```

53.4. voice vlan mac-address

Данная команда используется для добавления определенного пользователем OUI (уникального идентификатора организации) голосового устройства. Для удаления определенного пользователем OUI голосового устройства воспользуйтесь формой **no**.

voice vlan mac-address *MAC-ADDRESS MASK* **[description** *TEXT***]**

no voice vlan mac-address *MAC-ADDRESS MASK*

Параметры

MAC-ADDRES	Укажите MAC-адрес OUI.
MASK	Укажите соответствующую битовую маску MAC-адреса OUI.
description *TEXT*	(Опционально) Укажите описание определенного пользователем 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 определенного пользователем OUI голосового устройства. OUI используется для идентификации голосового трафика с помощью функции Voice VLAN. Если MAC-адреса источника полученных пакетов соответствуют любому из шаблонов OUI, полученные пакеты распознаются как голосовые пакеты.

Определенный пользователем OUI не может совпадать с OUI по умолчанию. OUI по умолчанию не может быть удален.

Пример

В данном примере показано, как добавить определенный пользователем OUI для голосового устройства.

```
Switch# configure terminal
Switch(config)#voice vlan mac-address 00-02-03-00-00-00 FF-FF-FF-00-00-00
description User1
Switch(config)#
```

53.5. voice vlan mode

Данная команда используется для включения автоматического изучения порта в качестве Member-порта Voice VLAN. Для отключения автоматического изучения воспользуйтесь формой **no**.

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 – **auto** и **untag**.

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 голосовое устройство через OUI, он автоматически присоединится к Voice VLAN как тегированный порт. Если голосовое 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 голосовом устройстве через OUI, он автоматически присоединится к Voice VLAN как нетегированный порт. Если голосовое 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)#
```

53.6. voice vlan qos

Данная команда используется для настройки приоритета CoS для входящего трафика Voice VLAN. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

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)#
```

53.7. show voice vlan

Данная команда используется для отображения настроек Voice VLAN.

show voice vlan [interface [*INTERFACE-ID* **[, | -]]]**

show voice vlan {device | lldpmed device} [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface	(Опционально) Укажите, чтобы отобразить информацию о портах Voice VLAN.
INTERFACE-ID	(Опционально) Укажите интерфейс, который необходимо отобразить.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
device	(Опционально) Укажите, чтобы отобразить голосовые устройства, информация о которых была получена через OUI.
lldp-med device	(Опционально) Укажите, чтобы отобразить голосовые устройства, обнаруженные через LLDP-MED.

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 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           : ethernet 1/0/1-1/0/5
Dynamic Member Ports : ethernet 1/0/1-1/0/3
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 ethernet 1/0/1-5

Interface     State       Mode
------------  ----------  ------------
ethernet 1/0/1      Enabled     Auto/Tag
ethernet 1/0/2      Enabled     Manual
ethernet 1/0/3      Enabled     Manual
ethernet 1/0/4      Enabled     Auto/Untag
ethernet 1/0/5      Disabled    Manual

Switch#
```

В данном примере показано, как отобразить распознанные голосовые устройства на Ethernet-портах 1/0/1-1/0/2.

```
Switch# show voice vlan device interface ethernet 1/0/1-2

Interface  Device Address     Start Time         Status
---------  ----------------- -----------------  -------
ethernet 1/0/1   00-03-6B-00-00-01  2012-03-19 09:00   Active
ethernet 1/0/1   00-03-6B-00-00-02  2012-03-20 10:09   Aging
ethernet 1/0/1   00-03-6B-00-00-05  2012-03-20 12:04   Active
ethernet 1/0/2   00-03-6B-00-00-0a  2012-03-19 08:11   Aging
ethernet 1/0/2   33-00-61-10-00-11  2012-03-20 06:45   Aging

Total Entries: 5

Switch#
```

В данном примере показано, как отобразить голосовые устройства, обнаруженные через LLDP-MED, на Ethernet-портах 1/0/1-1/0/2.

```
Switch# show voice vlan lldpmed device interface ethernet 1/0/1-2

Index                 : 1
Interface             : ethernet 1/0/1
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             : ethernet 1/0/2
Chassis ID Subtype : MAC Address
Chassis ID            : 00-E0-BB-00-00-12
Port ID Subtype      : Network Address
Port ID               : 172.18.1.2
Create Time           : 2012-03-20 11:00
Remain Time           : 105 Seconds

Total Entries: 2

Switch#
```

Приложение A. Записи системного журнала

В таблице ниже перечислены все записи и их соответствующие значения, появляющиеся в системном журнале коммутатора.

802.1X

	Описание записей журнала	Уровень
1	Описание события: ошибка аутентификации 802.1X. Сообщение в журнале: 802.1X authentication fails from (Username: <username>, Port: <interface-id>, MAC: <mac-address>) Описание параметров: username: пользователь, проходящий аутентификацию. interface-id: номер интерфейса коммутатора. mac-address: MAC-адрес аутентифицированного устройства.	Предупреждение
2	Описание события: успешная аутентификация 802.1X. Сообщение в журнале: 802.1X authentication succeeds from (Username: <username>, Port: <interface-id>, MAC: <mac-address>) Описание параметров: username: пользователь, проходящий аутентификацию. interface-id: имя интерфейса. mac-address: MAC-адрес аутентифицированного устройства.	Информационный

AAA

	Описание записей журнала	Уровень
1	Описание события: данный журнал будет сгенерирован, когда RADIUS назначит недопустимые атрибуты VLAN ID. Сообщение в журнале: Invalid vlan assignment by radius with vlan <vid>, port <interface-id> Описание параметров: vid: недопустимый назначенный VLAN ID, авторизованный RADIUS-сервером. interface-id: номер порта аутентифицированного клиента.	Предупреждение
2	Описание события: данный журнал будет сгенерирован, когда RADIUS назначит атрибуты недопустимого приоритета. Сообщение в журнале: Invalid port default 802.1p assignment by radius with 802.1p: <priority>, port < interface -id>	Предупреждение

	Описание параметров: priority: недопустимый назначенный приоритет, авторизованный RADIUS-сервером. interface-id: номер порта аутентифицированного клиента.	
3	Описание события: данный журнал будет сгенерирован, когда RADIUS назначит атрибуты недопустимой полосы пропускания. Сообщение в журнале: Invalid bandwidth assignment by radius with type <direction> rate <threshold>, port <interface -id> Описание параметров: direction: направление полосы пропускания: TX (исходящая) или RX (входящая). threshold: недопустимый назначенный порог полосы пропускания, авторизованный RADIUS-сервером. interface-id: номер порта аутентифицированного клиента.	Предупреждение
4	Описание события: данный журнал будет сгенерирован при запросе RADIUS назначения для порта 802.1X на основе MAC (режим узла (Host Mode) – Multi Auth). Сообщение в журнале: The port <interface -id> is set to 802.1X mac based, it does not support radius assignment. Описание параметров: interface-id: номер порта режима узла (Host Mode) аутентификации настроен как multi-auth.	Предупреждение
5	Описание события: данный журнал будет сгенерирован при запросе RADIUS назначения для router-порт IGMP Snooping. Сообщение в журнале: The port eth <interface -id> is set to a router port of igmp snooping, it does not support radius assignment. Описание параметров: interface-id: номер router-порта IGMP Snooping.	Предупреждение

Конфигурация/ПО/Журнал

	Описание записей журнала	**Уровень**
1	Описание события: ПО обновлено успешно. Сообщение в журнале: Firmware upgraded successfully via <session>! Описание параметров: session: сессия пользователя.	Информационный

2	Описание события: ошибка обновления ПО. Сообщение в журнале: Firmware upgraded failure via <session>! Описание параметров: session: сессия пользователя.	Предупреждение
3	Описание события: резервное копирование ПО выполнено успешно. Сообщение в журнале: Firmware backup successful via <session> Описание параметров: сессия пользователя.	Информационный
4	Описание события: ошибка резервного копирования ПО. Сообщение в журнале: Log Message:[Unit <unitID>,]Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Описание параметров: unitID: Unit ID. session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента. serverIP: IP-адрес сервера pathFile: путь и имя файла на сервере.	Предупреждение
5	Описание события: конфигурация успешно восстановлена. Сообщение в журнале: Configuration restore successful via <session> Описание параметров: session: сессия пользователя.	Информационный
6	Описание события: ошибка восстановления конфигурации. Сообщение в журнале: Configuration restore failure via <session>! Описание параметров: session: сессия пользователя.	Предупреждение
7	Описание события: резервное копирование конфигурации выполнено успешно. Сообщение в журнале: Configuration backup successfull via <session>. Описание параметров: session: сессия пользователя.	Информационный

8	Описание события: ошибка резервного копирования конфигурации. Сообщение в журнале: Configuration backup failure via <session>! Описание параметров: session: сессия пользователя.	Предупреждение
9	Описание события: конфигурация успешно сохранена. Сообщение в журнале: Configuration save successful.	Информационный
10	Описание события: ошибка сохранения конфигурации. Сообщение в журнале: Configuration save failure.	Предупреждение
11	Описание события: резервное копирование системного журнала выполнено успешно. Сообщение в журнале: System log backup successful via <session>. Описание параметров: session: сессия пользователя.	Информационный
12	Описание события: ошибка резервного копирования системного журнала. Сообщение в журнале: System log backup failure via <session>! Описание параметров: session: сессия пользователя.	Предупреждение

Interface

	Описание записей журнала	**Уровень**
1	Описание события: порт отключен. Сообщение в журнале: Port <port-type>< interface-id> link down Описание параметров: port-type: тип порта. interface-id: имя интерфейса.	Информационный
2	Описание события: порт включен. Сообщение в журнале: Port <port-type>< interface-id> link up, <link-speed> Описание параметров: port-type: тип порта. interface-id: имя интерфейса. link-speed: скорость соединения порта.	Информационный

LACP

	Описание записей журнала	Уровень
1	Описание события: группа агрегирования (Link Aggregation) включена. Сообщение в журнале: Trunk group< group_id > link up. Описание параметров: group_id: ID включенной группы агрегирования.	Информационный
2	Описание события: группа агрегирования (Link Aggregation) отключена. Сообщение в журнале: Trunk group< group_id > link down. Описание параметров: group_id: ID отключенной группы агрегирования.	Информационный
3	Описание события: Member-порт присоединился к группе агрегирования. Сообщение в журнале: Port <port_id> attach to Trunk group<group_id >. Описание параметров: port_id: ID порта, который был присоединен к группе агрегирования. group_id: ID группы агрегирования, к которой был присоединен порт.	Информационный
4	Описание события: Member-порт покинул группу агрегирования. Сообщение в журнале: Port <port_id> detach from Trunk group< group_id >. Описание параметров: port_id: ID порта, который покинул группу агрегирования. group_id: ID группы агрегирования, которую покинул порт.	Информационный

LBD

	Описание записей журнала	Уровень
1	Описание события: интерфейс обнаружил петлю Сообщение в журнале: Port <interface-id> LBD loop occurred. Port blocked. Описание параметров: interface-id: интерфейс, на котором обнаружена петля.	Критический

2	Описание события: интерфейс обнаружил петлю. Сообщение в журнале: Port <interface-id> LBD loop occurred. Port blocked at VID <vlan-id>. Описание параметров: interface-id: интерфейс, на котором обнаружена петля. vlan-id: VLAN, в которой обнаружена петля.	Критический
3	Описание события: восстановление режима обнаружения петли на интерфейсе. Сообщение в журнале: Port <interface-id> LBD loop recovered. Loop detection restarted. Описание параметров: interface-id: интерфейс, на котором обнаружена петля.	Информационный
4	Описание события: восстановление режима обнаружения петли на интерфейсе. Сообщение в журнале: Port <interface-id> LBD Port at VID <vlan-id> recovered. Loop detection restarted. Описание параметров: interface-id: интерфейс, на котором обнаружена петля. vlan-id: VLAN, в которой обнаружена петля.	Информационный
5	Описание события: интерфейс обнаружил петлю в режиме Port-Based. Сообщение в журнале: Port <interface-id> LBD loop occurred. Port not blocked as a result of NONE action mode. Описание параметров: interface-id: интерфейс, на котором обнаружена петля.	Критический
6	Описание события: интерфейс обнаружил петлю в режиме VLAN-Based. Сообщение в журнале: Port <interface-id> LBD port VID <vlan-id> loop occurred. Port not blocked as a result of NONE action mode. Описание параметров: interface-id: интерфейс, на котором обнаружена петля. vlan-id: VLAN, в которой обнаружена петля.	Критический

Login/Logout CLI

	Описание записей журнала	**Уровень**
1	Описание события: успешный вход через Telnet.	Информационный

	Сообщение в журнале: Successful login through Telnet (User: <username>, IP: <ipaddr>) Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	
2	Описание события: не удалось выполнить вход через Telnet. Сообщение в журнале: Login failed through Telnet (IP: <ipaddr>) Описание параметров: ipaddr: IP-адрес клиента.	Предупреждение
3	Описание события: время сессии Telnet истекло. Сообщение в журнале: Telnet session timed out (IP: <ipaddr>) Описание параметров: ipaddr: IP-адрес клиента.	Информационный
4	Описание события: выход через Telnet. Сообщение в журнале: Logout through Telnet (IP: <ipaddr>) Описание параметров: ipaddr: IP-адрес клиента.	Информационный

MSTP Debug Enhancement

	Описание записей журнала	**Уровень**
1	Описание события: Spanning Tree Protocol включен. Сообщение в журнале: Spanning Tree Protocol is enabled.	Информационный
2	Описание события: Spanning Tree Protocol отключен. Сообщение в журнале: Spanning Tree Protocol is disabled.	Информационный
3	Описание события: используется для записи события изменения топологии экземпляра MSTP. Сообщение в журнале: Topology changed (Instance : < Instance-id >, port: <interface_id>) Описание параметров: Instance-id: ID MST-экземпляра. Значение экземпляра по умолчанию равно 0, CIST. interface_id: номер порта, который обнаруживает или получает информацию об изменении топологии.	Информационный
4	Описание события: используется для записи нового выбранного корневого моста (Root Bridge). Сообщение в журнале: New Root bridge selected (MAC:	Информационный

	<macaddr> Priority :< priority>) Описание параметров: macaddr: MAC-адрес системы моста. priority: значение приоритета моста должно быть кратно 4096.	
5	Описание события: используется для записи события изменения топологии STP/RSTP. Сообщение в журнале: Topology changed (port : <interface_id>) Описание параметров: Interface_id: номер порта, который обнаруживает событие.	Информационный

Peripheral

	Описание записей журнала	**Уровень**
1	Описание события: вентилятор восстановлен. Сообщение в журнале: Right Fan <fan-descr> back to normal. Описание параметров: fan-descr: ID вентилятора и позиция.	Критический
2	Описание события: вентилятор вышел из строя. Сообщение в журнале: Right Fan <fan-descr> failed. Описание параметров: fan-descr: ID вентилятора и позиция.	Критический
3	Описание события: датчик температуры показывает критическое значение. Сообщение в журнале: Temperature exceeds the thresholds.	Критический
4	Описание события: температура вернулась к нормальному значению. Сообщение в журнале: Temperature recover.	Критический

Port Security

	Описание записей журнала	**Уровень**
1	Описание события: превышено максимальное количество адресов на порту. Сообщение в журнале: Port security violation (Port:<interface-id>). Описание параметров:	Предупреждение

	interface-id: имя интерфейса.	
2	Описание события: превышено максимальное количество адресов в системе. Сообщение в журнале: Limit on system entry number has been exceeded.	Предупреждение

SNMP

	Описание записей журнала	Уровень
1	Описание события: получен запрос SNMP с неверной строкой сообщества. Сообщение в журнале: SNMP request received with invalid <string>. Описание параметров: string: неверное имя сообщества или модель безопасности.	Предупреждение

Storm Control

	Описание записей журнала	Уровень
1	Описание события: возникновение шторма. Сообщение в журнале: <broadcast | multicast | unicast> storm is occurring on <interface-id>. Описание параметров: broadcast: шторм, возникший из-за широковещательных пакетов (DA = FF:FF:FF:FF:FF:FF). multicast: шторм, возникший из-за многоадресных пакетов, включая известные и неизвестные пакеты 2 уровня, пакеты с известным и неизвестным IP. unicast: шторм, возникший из-за одноадресных пакетов, включая известные и неизвестные пакеты. interface-id: ID интерфейса, на котором возник шторм.	Предупреждение
2	Описание события: соединение на порту прервано из-за возникновения шторма. Сообщение в журнале: <interface-id> is currently shutdown due to the <broadcast | multicast | unicast> storm. Описание параметров: interface-id: ID интерфейса, находящегося в состоянии Error-Disabled из-за шторма.	Предупреждение

	broadcast: интерфейс отключен из-за шторма широковещательных пакетов. multicast: интерфейс отключен из-за шторма многоадресных пакетов. unicast: интерфейс отключен из-за шторма одноадресных пакетов, включая известные и неизвестные пакеты.	

Telnet

	Описание записей журнала	**Уровень**
1	Описание события: успешный вход через Telnet. Сообщение в журнале: Successful login through Telnet (User: <username>, IP: <ipaddr>) Описание параметров: ipaddr: IP-адрес Telnet-клиента. username: имя пользователя, используемое для входа на Telnet-сервер.	Информационный
2	Описание события: не удалось выполнить вход через Telnet. Сообщение в журнале: Login failed through Telnet (IP: <ipaddr>) Описание параметров: ipaddr: IP-адрес Telnet-клиента.	Предупреждение
3	Описание события: выполнен выход через Telnet. Сообщение в журнале: Logout through Telnet (IP: <ipaddr>) Описание параметров: ipaddr: IP-адрес Telnet-клиента.	Информационный
4	Описание события: время сессии Telnet истекло. Сообщение в журнале: Telnet session timed out (IP: <ipaddr>). Описание параметров: ipaddr: IP-адрес Telnet-клиента.	Информационный

Web

	Описание записей журнала	**Уровень**
1	Описание события: успешный вход через Web. Сообщение в журнале: Successful login through Web (IP: <ipaddr>). Описание параметров:	Информационный

	ipaddr: IP-адрес HTTP-клиента.	
2	Описание события: не удалось войти через Web. Сообщение в журнале: Login failed through Web (IP: <ipaddr>). Описание параметров: ipaddr: IP-адрес HTTP-клиента.	Предупреждение
3	Описание события: выполнен выход через Web. Сообщение в журнале: Logout through Web (IP: <ipaddr>). Описание параметров: ipaddr: IP-адрес HTTP-клиента.	Информационный

Приложение Б. Записи trap-сообщений

Таблица ниже содержит все возможные записи trap-сообщений и их соответствующие значения, встречающиеся на коммутаторе.

802.1X

	Сообщение trap	Описание	OID
1	pnacAuthNotifyAuthSuccess	Хост прошел аутентификацию 802.1X. Вариабельные привязки: (1) networkPortAuthPortNumber (2) networkPortAuthVlan (3) networkPortAuthMac (4) networkPortAuthUserName	1.3.6.1.4.1.1 71.11.139.10 00.8.2.7.0.1
2	pnacAuthNotifyAuthFailure	Хост не прошел аутентификацию 802.1X. Вариабельные привязки: (1) networkPortAuthPortNumber (2) networkPortAuthVlan (3) networkPortAuthMac (4) networkPortAuthUserName (5) networkPortAuthFailReason	1.3.6.1.4.1.1 71.11.139.10 00.8.2.7.0.2

DHCP Server Screen Prevention

	Сообщение trap	Описание	OID
1	dhcpSerScrAttackDetect	Если функция DHCP Server Screen включена, trap-сообщения будут отправлены при получении каждого пакета ложного DHCP-сервера. Вариабельные привязки: (1) dhcpSerScrLogVlanID (2) dhcpSerScrLogIPAddr (3) dhcpSerScrLogMacAddr (4) dhcpSerScrLogOccurrence	1.3.6.1.4.1.17 1.11.139.100 0.8.7.3.0.1

ErrDisable

	Сообщение trap	Описание	OID
1	errDisNotifyPortDisabledAssert	Порт перешел в состояние Error-Disabled. Вариабельные привязки: (1) errDisIfStatusPortIndex (2) errDisIfStatusVlanIndex (3) errDisPortReason	1.3.6.1.4.1.171.11.139.10.00.2.13.8.0.1
2	errDisNotifyPortDisabledClear	Порт возвращается в исходное состояние по истечению определенного интервала времени. Вариабельные привязки: (1) errDisIfStatusPortIndex (2) errDisIfStatusVlanIndex (3) errDisPortReason	1.3.6.1.4.1.171.11.139.10.00.2.13.8.0.2
3	errDisNotifyVlanDisabledAssert	Порт перешел в состояние возникновения петли в VID. Вариабельные привязки: (1) errDisIfStatusPortIndex (2) errDisIfStatusVlanIndex (3) errDisPortReason	1.3.6.1.4.1.171.11.139.10.00.2.13.8.0.3
4	errDisNotifyVlanDisabledClear	Порт в VID возвращается в исходное состояние по истечению определенного интервала времени. Вариабельные привязки: (1) errDisIfStatusPortIndex (2) errDisIfStatusVlanIndex (3) errDisPortReason	1.3.6.1.4.1.171.11.139.10.00.2.13.8.0.4

LACP

	Сообщение trap	Описание	OID
1	linkUp	SNMP-устройство в роли агента обнаружило, что один из каналов связи перешел из состояния «down» в какое-то	1.3.6.1.6.3.1.1.5.4

		другое состояние (за исключением состояния notPresent). Текущее состояние указано в привязке ifOperStatus. Вариабельные привязки: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	
2	linkDown	SNMP-устройство в роли агента обнаружило, что один из каналов связи перешел в состояние «down» из какого-то другого состояния (за исключением состояния notPresent). Предыдущее состояние указано в привязке ifOperStatus. Вариабельные привязки: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1. 1.5.3

LBD

	Сообщение trap	Описание	OID
1	lbdLoopOccur	Обнаружена петля. Вариабельные привязки: (1) lbdportIndex	1.3.6.1.4.1.1 71.11.139.10 00.4.4.4.0.1
2	lbdLoopRecover	Порт возвращается в исходное состояние по истечению определенного интервала времени. Вариабельные привязки: (1) lbdportIndex	1.3.6.1.4.1.1 71.11.139.10 00.4.4.4.0.2

LLDP

	Сообщение trap	Описание	OID

1	lldpRemoteTableChanged	Значение lldpStatsRemTableLastChangeTime изменилось. Оно может быть использовано NMS для запуска опросов обслуживания таблиц удаленных систем LLDP. Вариабельные привязки: (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.3.6.1.4.1.1 71.11.139.10 00.4.7.12.0.1
2	lldpXMedTopologyChangeDetected	Обнаружено изменение в топологии: к порту было подключено новое устройство, удаленное устройство было отключено или было отключено с дальнейшем подключением к другому порту. Вариабельные привязки: (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass	1.3.6.1.4.1.1 71.11.139.10 00.4.7.18.1
3	lldpChasisIdMatched	Сконфигурированный и полученный chasisId от соседнего устройства совпадают.	1.3.6.1.4.1.1 71.11.139.10 00.4.7.12.0.2
4	lldpSystenameMatched	Сконфигурированное и полученное имя системы от соседнего устройства совпадают. Вариабельные привязки: (1) lldpRemSysName	1.3.6.1.4.1.1 71.11.139.10 00.4.7.12.0.3
5	lldpManagementaddressMatched	Сконфигурированный и полученный адрес управления от соседнего устройства совпадают. Полученный повторяющийся адрес управления отправляется с OID в качестве индекса. Следовательно, lldpRemManAddrIfId отправляется в поле значения. Вариабельные привязки: (1) lldpRemManAddr	1.3.6.1.4.1.1 71.11.139.10 00.4.7.12.0.4

6	lldpPVIDNotMatched	VLAN ID порта двух систем подключенных к одному каналу, отличается. Вариабельные привязки: (1) lldpXdot1RemPortVlanId	1.3.6.1.4.1.171.11.139.10.00.4.7.12.0.5
7	lldpVlannameNotMatched	Имя VLAN двух систем, подключенных к одному каналу, отличается. Вариабельные привязки: (1) lldpXdot1RemVlanName	1.3.6.1.4.1.171.11.139.10.00.4.7.12.0.6
8	lldpProtocolIDNotMatched	Протокол идентификации информации (например, Spanning Tree Protocol, Link Aggregation Protocol, Proprietary protocol) двух систем, подключенных к одному каналу, отличается. Вариабельные привязки: (1) lldpXdot1RemProtocolId	1.3.6.1.4.1.171.11.139.10.00.4.7.12.0.7
9	lldpLAstatusNotMatched	Настройка группы агрегирования двух систем, подключенных к одному каналу, отличается. Вариабельные привязки: (1) lldpXdot3RemLinkAggStatus	1.3.6.1.4.1.171.11.139.10.00.4.7.12.0.8
10	lldpMaxFrameSizeNotMatched	Конфигурация максимального размера кадра двух систем, подключенных к одному каналу, отличается. Вариабельные привязки: (1) lldpXdot3RemMaxFrameSize	1.3.6.1.4.1.171.11.139.10.00.4.7.12.0.9
11	lldpMAUTypeNotMatched	Operational MAU Type двух систем, подключенных к одному каналу связи, отличается. Вариабельные привязки: (1) lldpXdot3RemPortOperMauType	1.3.6.1.4.1.171.11.139.10.00.4.7.12.0.10

MSTP

	Сообщение trap	Описание	OID
1	stpNewRootTrap	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. Вариабельные привязки: (1) deviceInfoMACAddress (2) mstMstiBridgeRegionalRoot	1.3.6.1.4.1.1 71.11.139.10 00.4.3.6.0.1
2	stpTopologyChgTrap	Мост отправляет trap-собщение, когда какой-то из его настроенных портов переходит из состояния Learning в состояние Forwarding или из состояния Forwarding в состояние Blocking. Данное trap-собщение не отправляется повторно. Отправка данного trap-собщения является опциональной. Вариабельные привязки: (1) deviceInfoMACAddress (2) mstMstiTopChanges	1.3.6.1.4.1.1 71.11.139.10 00.4.3.6.0.2

Peripheral

	Сообщение trap	Описание	OID
1	envTrapFanFailed	Вентилятор вышел из строя. Вариабельные привязки: (1) environmentFanId	1.3.6.1.4.1.1 71.11.139.10 00.2.2.5.0.1
2	envTrapFanRecover	Восстановление вентилятора.	1.3.6.1.4.1.1

		Вариабельные привязки: (1) environmentFanId	71.11.139.10 00.2.2.5.0.2
3	envTrapTemperatureExceed	Температура превышает пороговые значения. Вариабельные привязки: (1) environmentTempCurrent	1.3.6.1.4.1.1 71.11.139.10 00.2.2.5.0.3
4	envTrapTemperatureRecover	Восстановление температуры. Вариабельные привязки: (1) environmentTempCurrent	1.3.6.1.4.1.1 71.11.139.10 00.2.2.5.0.4

Port

	Сообщение trap	**Описание**	**OID**
1	linkUp	Соединение на порту установлено. Вариабельные привязки: (1) ifIndex (2) ifAdminStatus (3) ifOperStatu	1.3.6.1.4.1.1 71.11.139.10 00.3.3.1.7
2	linkDown	Соединение на порту прервано. Вариабельные привязки: (1) ifIndex (2) ifAdminStatus (3) ifOperStatu	1.3.6.1.4.1.1 71.11.139.10 00.3.3.1.8

Port Security

	Сообщение trap	**Описание**	**OID**
1	portSecurityVioAction	Если отправка trap-сообщений Port Security включена, trap-сообщения будут отправлены при обнаружении недопустимых MAC-адресов. Вариабельные привязки: (1) portSecurityPort (2) portSecurityVioCount	1.3.6.1.4.1.1 71.11.139.10 00.8.1.2.1.1. 4

RMON

	Сообщение trap	Описание	OID
1	risingAlarm	Запись уровня/типа alarm превысила заданный верхний порог. Вариабельные привязки: (1) alarmIndex (2) eventDescription (3) alarmVariable (4) alarmSampleType (5) alarmValue (6) alarmRisingThreshold	1.3.6.1.4.1.1 71.11.139.10 00.3.4.1
2	fallingAlarm	Запись уровня/типа alarm снизилась до заданного нижнего порога. Вариабельные привязки: (1) alarmIndex (2) eventDescription (3) alarmVariable (4) alarmSampleType (5) alarmValue (6) alarmFallingThreshold	1.3.6.1.4.1.1 71.11.139.10 00.3.4.2

Start

	Сообщение trap	Описание	OID
1	coldStart	Повторная инициализация SNMPv2-устройства в роли агента и возможное изменение его настроек.	1.3.6.1.4.1.1 71.11.139.10 00.3.3.1.9
2	warmStart	Повторная инициализация SNMPv2-устройства в роли агента с неизмененной конфигурацией.	1.3.6.1.4.1.1 71.11.139.10 00.3.3.1.10

Storm Control

	Сообщение trap	Описание	OID
1	stormCtrlTrapsStormOccur	Данное trap-сообщение будет отправлено при возникновении или обнаружении шторма. Вариабельные привязки: (1) stormCtrlIndex	1.3.6.1.4.1.1 71.11.139.10 00.8.16.1.1.6 .0.1
2	stormCtrlTrapsStormClear	Данное trap-сообщение будет отправлено при устранении шторма. Вариабельные привязки: (1) stormCtrlIndex	1.3.6.1.4.1.1 71.11.139.10 00.8.16.1.1.6 .0.2

Приложение B. Назначение атрибутов RADIUS

На коммутаторах DXS-1210 назначение атрибутов RADIUS используется в следующих модулях: Console, Telnet, SSH, Web, 802.1X, JWAC, WAC и управление доступом на основе MAC.

Ниже представлены следующие атрибуты RADIUS:

- Входящая/исходящая полоса пропускания (Ingress/Egress Bandwidth)
- Приоритет по умолчанию 802.1p
- VLAN

Для того чтобы RADIUS-сервер назначил **входящую/исходящую полосу пропускания**, необходимо сконфигурировать соответствующие параметры на сервере. В таблице ниже приведены параметры для полосы пропускания.

Атрибуты для производителя (Vendor-Specific attributes):

Атрибут для производителя	**Описание**	**Значение**	**Использование**
Vendor-ID	Определяет производителя	171 (DLINK)	Обязательно
Vendor-Type	Определяет атрибут	2 (для входящей полосы) 3 (для исходящей полосы)	Обязательно
Attribute-Specific Field	Используется для назначения полосы пропускания порта	Unit (Kbits)	Обязательно

Если пользователь сконфигурировал атрибут полосы пропускания на RADIUS-сервере (например, входящая полоса пропускания 1000 кбит/с) и аутентификация 802.1X прошла успешно, устройство назначит полосу пропускания пользователю в соответствии со значением на RADIUS-сервере. Однако если пользователь не сконфигурировал атрибут полосы пропускания и аутентификация проходит успешно, устройство не назначит пользователю полосу пропускания. Если атрибут полосы пропускания установлен на «0», для эффективной полосы пропускания будет установлен параметр no_limited. Если атрибут полосы пропускания установлен на значение ниже нуля или выше максимального поддерживаемого значения, полоса пропускания игнорируется.

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.

Атрибуты для производителя (Vendor-Specific attributes):

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 сконфигурировал атрибут приоритета 802.1p на RADIUS-сервере (например, приоритет 7) и аутентификация 802.1X прошла успешно, устройство назначит порту приоритет по умолчанию в соответствии со значением на RADIUS-сервере. Однако если пользователь не сконфигурировал атрибут приоритета и аутентификация проходит успешно, устройство не назначит порту приоритет. Если атрибут приоритета на RADIUS-сервере установлен на значение вне диапазона (>7), он не будет установлен на устройстве.

Для того чтобы RADIUS-сервер назначил **VLAN**, необходимо сконфигурировать соответствующие параметры на сервере. Для назначения VLAN RFC 3580 определяет следующие атрибуты в пакетах RADIUS.

Параметры для VLAN:

RADIUS Tunnel Attribute	Описание	Значение	Использование
Tunnel-Type	Этот атрибут указывает туннельный протокол, который нужно использовать в качестве инициатора или терминатора туннеля	13 (VLAN)	Обязательно
Tunnel-Medium-Type	Атрибут указывает используемую транспортную среду	6 (802)	Обязательно
Tunnel-Private-Group-ID	Атрибут указывает групповой ID для определенной туннельной сессии	ASCII (VID)	Обязательно

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 В, «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 D-Link, приведен в таблице ниже.

Атрибуты аутентификации RADIUS:

Номер	Атрибут IETF
1	User-Name
2	User-Password
18	Reply-Message
24	State
26	Vendor-Specific
27	Session-Timeout
29	Termination-Action
64	Tunnel-Type
65	Tunnel-Medium-Type
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID

Приложение Д. Информация о ERPS

Только Hardware-Based (аппаратный) ERPS (внешний PHY) поддерживает функцию быстрого прерывания связи (Fast Link Drop Interrupt) со временем восстановления 50 мс.

Наименование модели	**ERPS**	**Порт 1-8**	**Порт 9-12**
DXS-1210-12TC	Hardware-based	V	V
	Software-based		

Наименование модели	**ERPS**	**Порт 1-8**	**Порт 9-12**
DXS-1210-12SC	Hardware-based	V	V
	Software-based		

Наименование модели	**ERPS**	**Порт 1-8**	**Порт 9-10**
DXS-1210-10TS	Hardware-based	V	V
	Software-based		

Наименование модели	**ERPS**	**Порт 1-8**	**Порт 9-16**
DXS-1210-16TC	Hardware-based	V	V
	Software-based		