# Руководство пользователя (CLI)

*Сокращенный вариант*

## Серия DXS-3600

Управляемые стекируемые 10-гигабитные коммутаторы 3 уровня

Версия 2.40

# Оглавление

# 1. Введение

Описание команд в данном руководстве основано на программном обеспечении версии 2.40 с образом Enhanced Image (EI). Представленный здесь список является подмножеством команд, поддерживаемых коммутаторами серии DXS-3600.

## *1.1. Аудитория*

Руководство предназначено для сетевых администраторов и других IT-специалистов, использующих для управления коммутатором интерфейс командной строки (CLI). Это основной интерфейс управления коммутаторами серии DXS-3600(далее "коммутатор"). Настоящее руководство рассчитано на пользователей, знакомых с основными принципами работы Ethernet и организацией современных локально-вычислительных сетей (ЛВС).

## *1.2. Условные обозначения*

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

**Предупреждения и примечания**

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.

**Описание команд**

Информация по каждой команде в данном руководстве представлена в следующем виде:

- **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.

## *1.3. 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 пять уровней привилегий учетной записи пользователя:

- **Basic User**– 1-й уровень привилегий. Данный уровень учетной записи обладает самым низким приоритетом среди учетных записей и позволяет пользователю получить доступ к просмотру базовой информации о системе.
- **Advanced User**– 3-й уровень привилегий. Данный уровень учетной записи позволяет менять настройки управления терминалом. Пользователь может получить доступ к ограниченной информации, не относящейся к безопасности.
- **Power User**– 8-й уровень привилегий. На данном уровне учетной записи доступно меньше команд, чем на уровне Operator. Поддерживаются команды конфигурирования, за исключением команд уровня Operator и Administrator.
- **Operator**– 12-й уровень привилегий. Данный уровень учетной записи позволяет менять локальные и глобальные настройки, не относящиеся к безопасности, например, настройки учетных записей пользователей, учетных записей SNMP и т.д.
- **Administrator**– 15-й уровень привилегий. Учетная запись уровня Administrator позволяет получить доступ ко всей информации о системе и системным настройкам, доступным в данном руководстве.

Интерфейс командной строки (CLI) использует несколько режимов в следующем иерархическом порядке.

Базовые режимы:

- **User EXEC Mode** (Пользовательский режим EXEC);
- **Privileged EXEC Mode** (Привилегированный режим EXEC);
- **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 привилегий, включая **Advanced User**, **Power User**, **Operator** и **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 Advanced User, Power User, 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.

Таблица 1.1 Доступные командные режимы и уровни привилегий:

| **Режим ввода команд / Уровень привилегий** | **Описание** |
|---|---|
| User EXEC Mode / Уровень Basic User | Самый низкий уровень приоритета среди пользовательских учетных записей. Доступ только к просмотру базовых настроек системы. |
| Privileged EXEC Mode / Уровень Advanced User | На данном уровне есть доступ к настройкам управления терминалом. Пользователь может получить доступ к просмотру ограниченной информации, не относящейся к безопасности. |
| Privileged EXEC Mode / Уровень Power User | Меньше команд, чем на уровне Operator. Доступны команды конфигурирования, за исключением команд уровня Operator и Administrator. |
| 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. |
| VLAN Configuration Mode | Режим настройки VLAN. |

| | |
|---|---|
| IP Access-List Configuration Mode | Режим настройки IP Access-List. |

**User EXEC Mode с базовым уровнем доступа Basic User**

Есть доступ к базовой информации о настройках. В данный режим можно войти с учетной записью Basic User.

**Privileged EXEC Mode с расширенным уровнем доступа Advanced User**

Режим предназначен для просмотра базовых настроек системы и позволяет пользователям осуществлять настройки сеансов локального терминала и выполнять базовую проверку сетевых подключений. Пользователь не может получить доступ к информации, относящейся к безопасности. В данный режим можно войти с учетной записью уровня Advanced User.

**Privileged EXEC Mode с уровнем доступа Power User**

В этом режиме пользователю доступно меньше команд, чем пользователю с учетной записью уровня Operator. Поддерживаются команды 'config' за исключением команд уровня Operator и уровня Administrator. Вход в данный режим можно получить, имея 8-й уровень привилегий.

**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.

**Режим глобальной конфигурации (Global Configuration Mode)**

Данный режим позволяет вносить изменения в глобальные настройки всей системы. Для входа в режим требуется учетная запись уровня Advanced User, Power User, 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 в режим 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.

**Режим конфигурирования интерфейса (Interface Configuration Mode)**

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.

**Режим конфигурирования интерфейса VLAN (VLAN Interface Configuration Mode)**

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)#
```

## *1.4. Создание пользовательской учетной записи*

По умолчанию на устройстве нет учетной записи пользователя. В целях безопасности рекомендуется создать учетную запись для управления интерфейсом коммутатора. Этот раздел поможет пользователю создать учетную запись с помощью интерфейса командной строки.

Рассмотрим следующий пример.

```
Switch# enable
Switch# configure terminal
Switch(config)# username admin password admin
Switch(config)# username admin privilege 15
Switch(config)# line console
Switch(config-line)# login local
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 admin password admin** создается учетная запись пользователя с именем *admin* и паролем *admin.*
- Команда **username admin privilege 15** назначает 15-й уровень привилегий для учетной записи admin.
- Команда **line console** позволяет получить доступ к режиму конфигурации строки интерфейса.
- Команда **login local** объявляет коммутатору, что для получения доступа к консоли пользователю необходимо ввести учетные данные из локальной базы.

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-3600-32S TenGigabit Ethernet Switch

                              Command Line Interface
                             Firmware: Build 2.40.041
          Copyright(C) 2015 D-Link Corporation. All rights reserved.

User Access Verification

Username:admin
Password:*****

Switch#
```

## *1.5. 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.

## *1.6. Сообщения об ошибке*

Если коммутатор не распознает введенную команду, на экране появятся сообщения об ошибке с основной информацией о проблеме.

Таблица 1.2 Сообщения об ошибках с описанием проблемы.

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

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

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

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

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

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

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

## *1.7. Функции редактирования*

Интерфейс командной строки коммутатора поддерживает следующие клавиши для редактирования.

Таблица 1.3 Доступные клавиши с описанием возможностей.

| **Клавиша** | **Описание** |
|---|---|
| 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 будет автоматически заменен новым. |
| Return | Прокручивает вниз к следующей строке или используется для ввода команды. |
| Пробел | Прокручивает вниз на следующую страницу. |
| ESC | Выход из отображаемой страницы. |

## *1.8. 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 # DEVICE
# DEVICE
configure terminal
end

# AAA

configure terminal
# AAA START
```

```
no aaa new-model
# AAA END
end

Switch#
```

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

```
Switch#show running-config | include # DEVICE
# DEVICE

Switch#
```

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

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

Current configuration : 56102 bytes

#------------------------------------------------------------------------------
#                   DXS-3600-32S TenGigabit Ethernet Switch
#                               Configuration
#
#                           Firmware: Build 2.40.041
#           Copyright(C) 2015 D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------------

# STACK

##  stacking config information
##   #Box                  Prio-
##   #ID    Type      Exist rity
##   #--- ----------- ----- -----
##   #  1 DXS-3600-32S exist 32
##   #  2 DXS-3600-16S no
##   #  3 NOT_EXIST no
end
end

configure terminal
end

# AAA

configure terminal
# AAA START
no aaa new-model
# AAA END
end

Switch#
```

# 2. Базовые команды CLI

## *2.1. help*

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

**help**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

User 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              reconfig            rename

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# ip access-list standard ?

<1-1999>             Standard IP access-list number
WORD                 Access-list name

Switch# ip access-list standard
```

## *2.2. enable*

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

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

**Параметры**

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

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Privileged EXEC Mode.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

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

**Пример**

В данном примере показано, как перейти в режим Privileged EXEC.

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

## *2.3. disable*

Данная команда используется для изменения уровня привилегий пользователя на более низкий.

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

**Параметры**

| | |
|---|---|
| *PRIVILEGE-LEVEL* | Указывается уровень привилегий. Если значение не задано, используется уровень 1. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.
Privileged EXEC Mode.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для изменения текущего уровня привилегий пользователя на более низкий. Если на данном уровне установлен пароль, то вводить его не требуется.

**Пример**

В данном примере показано, как выйти из системы.

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

## *2.4. configure terminal*

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

**configure terminal**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

Privileged EXEC Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется для входа в режим глобальной конфигурации.

**Пример**

В данном примере показан процесс входа в режим глобальной конфигурации.

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

## *2.5. login (EXEC)*

Данная команда используется для настройки имени пользователя.

**login**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Privileged EXEC Mode.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

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

**Пример**

В данном примере показан процесс входа в учетную запись с именем пользователя «user1».

```
Switch# login

Username: user1
Password: xxxxx

Switch#
```

## *2.6. login (Line)*

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

**login [local]**

**no login**

**Параметры**

| | |
|---|---|
| **login** | Укажите, чтобы включить требование авторизации при входе в систему. |
| **local** | (Опционально) Укажите, чтобы использовать локальную базу данных при аутентификации. |

**По умолчанию**

По умолчанию для доступа через **консоль** учетные данные не заданы.

По умолчанию настроен метод входа для доступа по **Telnet** (с паролем).

По умолчанию настроен метод входа для доступа по **SSH** (с паролем).

**Режим ввода команды**

Line Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

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

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

Для доступа по SSH используется 3 типа аутентификации:

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

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

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

  - Если авторизация отключена, имя пользователя и пароль игнорируются. Ввод учетных данных осуществляется на уровне 1.

  - Если выбрана опция **username and password**, введите имя пользователя и пароль, сконфигурированные командой **username.**

  - При выборе опции **password** имя пользователя игнорируется, но требуется ввод пароля, используемого в команде **password,** для входа в систему на уровне 1

**Пример**

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

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

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

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

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

```
Switch#login

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

Switch#
```

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

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

В данном примере показан процесс конфигурации метода входа login local.

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

## *2.7. logout*

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

**logout**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.
Privileged EXEC Mode.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

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

**Пример**

В данном примере показан процесс выхода из системы.

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

## *2.8. end*

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

**end**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для возврата 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 1/1
Switch(config-if)#end
Switch#
```

## *2.9. exit*

Данная команда используется для выхода из текущего режима конфигурации 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 EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для выхода из текущего режима конфигурации 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)#
```

## *2.10. show history*

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

**show history**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

User 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#
```

## *2.11. password-recovery*

Данная команда используется для восстановления настроек пароля. Используйте данную команду в режиме сброса конфигурации (Reset Configuration Mode).

**password-recovery**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

Reset Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

В некоторых ситуациях администратору необходимо обновить учетные данные пользователя, потому что пароль от учетной записи был утерян. Для этого администратор должен войти в режим **Reset Configuration Mode.** Для получения дополнительной информации о входе в данный режим свяжитесь с представителем технической поддержки.

После входа в режим сброса конфигурации необходимо использовать команду **password-recovery** и следовать предложенным инструкциям по восстановлению пароля.

Данная команда позволяет:

- обновить существующую учетную запись путем ввода существующего имени пользователя и нового пароля или добавить новую учетную запись с уровнем привилегий 15. Новая учетная запись не может быть создана, если превышено максимально возможное число пользовательских учетных записей;
- обновить действующий пароль для уровня привилегий Administrator;
- отключить функцию AAA для возможности локальной аутентификации в системе.

Обновленные настройки будут сохранены в текущем файле конфигурации. Перед перезагрузкой коммутатор предложит администратору подтвердить сохранение текущей конфигурации (Running Configuration) в качестве конфигурации при загрузке (Startup Configuration).

**Пример**

В данном примере показан процесс использования функции восстановления пароля.

```
Switch(reset-config)# password-recovery

This command will guide you to do the password recovery procedure.
Do you want to update the user account? (y/n) [n]y
Please input user account: user1
Please input user password:
Do you want to update the enable password for privilege level 15? (y/n) [n]y
Please input privilege level 15 enable password:
Do you want to disable AAA function to let the system do the local authentication?
(y/n) [n] y

Switch(reset-config)#
```

## *2.12. show environment*

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

**show environment [fan | power | temperature]**

**Параметры**

| | |
|---|---|
| **fan** | (Опционально) Отображение детальной информации о состоянии вентиляторов. |
| **power** | (Опционально) Отображение детальной информации о питании. |

| | |
|---|---|
| **temperature** | (Опционально) Отображение детальной информации о температуре. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Если параметр не задан, отображаться будут все типы информации.

**Пример**

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

```
Switch#show environment

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

Detail Fan Status:
-------------------------------------------------------------
  Fan 1 (OK)     Fan 2 (OK)     Fan 3 (OK)

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

Switch#
```

**Отображение параметров**

| | |
|---|---|
| **Power Status** | **in-operation**: источник питания работает нормально.<br>**failed:** источник питания не работает нормально.<br>**empty**: источник питания не подключен. |

## *2.13. show unit*

Данная команда позволяет получить общую информацию о системе.

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

**Параметры**

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

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для просмотра информации по устройствам стека. Если параметр UNIT-ID не указан, выводится информация по всем устройствам.

**Пример**

В данном примере показано отображение информации по устройствам в стеке.

```
Switch#show unit

Unit         Model Descr                              Model Name
----  ----------------------------------------  ------------------
 1     24P tenGigabitEthernet                    DXS-3600-32S

Unit         Serial-Number                Status        Up Time
----  --------------------------------  ---------  -----------------
 1     0123456789012                     ok         0DT1H45M53S

Unit   Memory     Total       Used        Free
----  --------  ----------  ----------  ----------
 1     DRAM     2097152 K    212913 K   1884239 K
 1     FLASH    1048064 K     13838 K   1034226 K

Switch#
```

## *2.14. show cpu utilization*

Данная команда позволяет получить информацию об использовании CPU.

**show cpu utilization**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

User 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 примере ниже показано получение информации о загрузке процессора.

```
Switch# show cpu utilization

CPU Utilization

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

Switch#
```

## *2.15. show version*

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

**show version**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

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

**Пример**

В данном примере показано отображение информации о коммутаторе.

```
Switch#show version

System MAC Address: 00-00-00-11-22-33

Unit ID    Module Name            Versions
-------  ------------------  ---------------------
   1      DXS-3600-32S         H/W:B1
                               Bootloader:1.10.009
                               Runtime:2.40.039

Switch#
```

## *2.16. environment temperature threshold*

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

**environment temperature threshold unit** *UNIT-ID* **thermal** *THERMAL-ID* **[high** *VALUE***] [low** *VALUE***]**

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

**Параметры**

| | |
|---|---|
| **unit** *UNIT-ID* | Укажите номер устройства (UNIT-ID). |
| **thermal** *THERMAL-ID* | Укажите идентификатор термодатчика. |
| **high** | (Опционально) Указывается верхняя граница температур в градусах Цельсия. Доступен диапазон от -100 до 200. |
| **low** | (Опционально) Указывается нижняя граница температур в градусах Цельсия. Доступен диапазон от -100 до 200. Нижняя граница не может быть выше верхней границы. |

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда позволяет настроить пороговые значения температуры окружающей среды внутри устройства, соответствующие нормальному диапазону рабочих температур, определенных для датчика. Нижняя граница температурного диапазона не может быть выше верхней. Настроенный диапазон должен быть в пределах минимума и максимума разрешенных температур, определенных для датчика. При превышении заданного порога будет отправлено уведомление.

**Пример**

В данном примере показан процесс настройки диапазона температур для термодатчика с ID 1 в устройстве Unit 1.

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

## *2.17. snmp-server enable traps environment*

Данная команда позволяет получать трапы о состоянии питания, температуре и работе вентиляторов.

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

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

**Параметры**

| | |
|---|---|
| **fan** | (Опционально) Укажите для получения трапов о состоянии вентиляторов, чтобы получать предупреждения о событиях (остановка вентилятора или восстановление работы вентилятора). |

| | |
|---|---|
| **power** | (Опционально) Укажите для получения трапов о состоянии питания, чтобы получать предупреждения о событиях (отказ питания или восстановление питания). |
| **temperature** | (Опционально) Укажите для получения трапов о температуре, чтобы получать предупреждение о событиях (превышение пороговых значений температуры или восстановление температуры). |

**По умолчанию**

По умолчанию поддержка трапов для данных параметров отключена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

В данном примере показан процесс включения трапов.

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

# 3. Команды 802.1X

## *3.1. clear dot1x counters*

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

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

**Параметры**

| | |
|---|---|
| **all** | Обнуление счетчиков 802.1X (диагностика, статистика и статистика сессии) на всех интерфейсах. |
| **interface** *INTERFACE-ID* | Обнуление счетчиков 802.1X (диагностика, статистика и статистика сессии) на определенном интерфейсе. Допустимыми интерфейсами являются физические порты (включая тип, номер в стеке и номер порта). |
| **,** | (Опционально) Используется для перечисления 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 показан процесс обнуления счетчиков 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 типа трафика на порту как однонаправленного (in) или двунаправленного (both). При использовании формы **no** команда вернет настройки по умолчанию.

**dot1x control-direction {both | in}**

**no dot1x control-direction**

**Параметры**

| | |
|---|---|
| **both** | Включение контроля трафика в двух направлениях. |

| | |
|---|---|
| **in** | Включение контроля трафика в одном направлении. |

**По умолчанию**

По умолчанию используется двунаправленный режим.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

Предположим, управление портом настроено как **auto**. Если направление задано как **both**, порт может принимать и передавать только пакеты EAPOL. Весь пользовательский трафик заблокирован до аутентификации. Если направление задано как **in**, в дополнение к приему и передаче пакетов EAPOL, порт может передавать пользовательский трафик, но не может получать его до аутентификации.

**Пример**

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

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

## *3.3. dot1x default*

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

**dot1x default**

**Параметры**

Нет.

**По умолчанию**

Данная опция отключена.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**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. При использовании формы **no** данная команда вернет настройки по умолчанию.

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

**no dot1x port-control**

**Параметры**

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

**По умолчанию**

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

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

Данная команда доступна только для конфигурации интерфейса физического порта.

Если управление портом настроено как **force-authorized**, то контроль трафика в обоих направлениях не осуществляется.

Если управление портом настроено как **auto**, то для контроля трафика в заданном направлении необходимо пройти процедуру аутентификации.

Если управление портом настроено как **force-unauthorized**, управление портом в указанном направлении заблокировано.

**Пример**

В данном примере показан процесс запрета любого доступа на Ethernet-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. При использовании формы **no** данная команда отключит функцию продвижения кадров dot1x PDU.

**dot1x forward-pdu**
**no dot1x forward-pdu**

**Параметры**
Нет.

**По умолчанию**
По умолчанию данная опция отключена**.**

**Режим ввода команды**
Interface Configuration Mode.

**Уровень команды по умолчанию**
Уровень 12.

**Использование команды**
Данная команда доступна только для конфигурации интерфейса физического порта. Команда работает, только если аутентификация dot1x на настраиваемом порту отключена. Принятые PDU будут перенаправлены либо с тегом, либо без тега в зависимости от настроек VLAN.

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

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

## *3.6. dot1x initialize*

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

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

**Параметры**

| | |
|---|---|
| **interface** *INTERFACE-ID* | Порт, на котором будет инициирована аутентификация. Доступными интерфейсами являются физические порты. |
| **,** | (Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Указывается для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы. |
| **mac-address** *MAC-ADDRESS* | Указывается 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 позволяет задать максимальное количество попыток для передачи клиенту запроса EAP (Extensive Authentication Protocol) от внутреннего сервера аутентификации, прежде чем инициировать повторную аутентификацию. При использовании формы **no** данная команда вернет настройки по умолчанию.

**dot1x max-req** *TIMES*

**no dot1x max-req**

**Параметры**

| | |
|---|---|
| *TIMES* | Число запросов, в которых коммутатор повторно передает кадр EAP запрашивающему устройству перед перезапуском процесса аутентификации. Диапазон допустимых значений: от 1 до 10. |

**По умолчанию**

По умолчанию используется значение 2.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

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

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

## *3.8. dot1x pae authenticator*

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

**dot1x pae authenticator**

**no dot1x pae authenticator**

**Параметры**

Нет.

**По умолчанию**

По умолчанию 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 аутентификации 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 интерфейса 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* | Указывается 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) Указывается для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы. |
| **mac-address** *MAC-ADDRESS* | Указывается 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. При использовании формы **no** данная команда отключит аутентификацию IEEE802.1X.

**dot1x system-auth-control**

**no dot1x system-auth-control**

**Параметры**

Нет.

**По умолчанию**

По умолчанию данная опция отключена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Функция аутентификации IEEE 802.1X не позволяет неавторизованным узлам получать доступ к сети. Используйте команду **dot1x system-auth-control** для глобального включения аутентификации IEEE 802.1X. Если аутентификация IEEE 802.1X включена, система будет аутентифицировать пользователя 802.1X на основе списка методов, указанных командой **aaa authentication dot1x default**.

**Пример**

В данном примере показан процесс включения глобальной аутентификации IEEE 802.1X.

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

## *3.11. dot1x timeout*

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

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

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

**Параметры**

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

**По умолчанию**

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

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

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

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда доступна только для конфигурации интерфейса физического порта.

**Пример**

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

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

## *3.12. show dot1x*

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

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

**Параметры**

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Опционально) Интерфейс или группа интерфейсов, для которых будет отображаться конфигурация dot1x. Если значение не указано, отображаться будет глобальная конфигурация. |
| **,** | (Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Указывается для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы. |

**По умолчанию**

Нет.

**Режим ввода команды**

User 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

Switch#
```

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

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

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

Switch#
```

## *3.13. show dot1x diagnostics*

Данная команда используется для просмотра результатов диагностики IEEE 802.1X. Если не задан определенный интерфейс, система выводит информацию по всем интерфейсам.

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

**Параметры**

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Опционально) Интерфейс или группа интерфейсов, для которых будут отображаться данные диагностики dot1x. 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) Указывается для обозначения диапазона интерфейсов. 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 для отображения результатов диагностики IEEE 802.1X. Если значение не указано, отображаться будут данные для всех интерфейсов. В противном случае отображаются данные диагностики для заданного интерфейса.

**Пример**

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

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

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

Switch#
```

## *3.14. show dot1x statistics*

Данная команда используется для просмотра статистики IEEE 802.1X. Если не задан определенный интерфейс, система выводит данные по всем интерфейсам.

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

**Параметры**

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Опционально) Интерфейс или группа интерфейсов, для которых будет отображаться статистика dot1x. Если значение не указано, отображаться будет информация для всех интерфейсов. |
| **,** | (Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Указывается диапазон интерфейсов. 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 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

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

Switch#
```

## *3.15. show dot1x session-statistics*

Данная команда используется для отображения статистики сессий IEEE 802.1X. Если не задан определенный интерфейс, система выводит данные по всем интерфейсам.

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

**Параметры**

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Опционально) Интерфейс или группа интерфейсов, для которых будет отображаться статистика сессии dot1x. Если значение не указано, отображаться будет информация для всех интерфейсов. |
| **,** | (Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Указывается для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

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

**Пример**

В 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

eth6/0/1 session statistic counters are following:
SessionOctetsRX                         : 0
SessionOctetsTX                         : 0
SessionFramesRX                         : 0
SessionFramesTX                         : 0
SessionId                               :
SessionAuthenticationMethod             : Remote Authentication Server
SessionTime                             : 0
SessionTerminateCause                   :SupplicantLogoff
SessionUserName                         :

Switch#
```

## *3.16. snmp-server enable traps dot1x*

Данная команда используется для включения отправки уведомлений SNMP для аутентификации 802.1X. При использовании формы **no** данная команда отключит отправку уведомлений SNMP.

**snmp-server enable traps dot1x**

**no snmp-server enable traps dot1x**

**Параметры**

Нет.

**По умолчанию**

По умолчанию данная функция отключена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Нет.

**Пример**

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

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

# 4. Команды ACL (Список управления доступом)

## *4.1. access-list resequence*

Данная команда используется для того, чтобы изменить нумерацию записей в списке доступа. При использовании формы **no** команда вернет настройки по умолчанию.

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

**no access-list resequence**

**Параметры**

| | |
|---|---|
| *NAME* | Укажите имя конфигурируемого списка доступа. Максимальное количество символов – 32. |
| *NUMBER* | Укажите номер конфигурируемого списка доступа. |
| *STARTING-SEQUENCE-NUMBER* | Укажите начальное значение, в соответствии с которым будут перегруппированы записи в списке. Значение по умолчанию – 10. Доступен диапазон значений от 1 до 65535. |
| *INCREMENT* | Укажите шаг для присвоения порядковых номеров. Значение по умолчанию – 10. Например, если значение шага равно 5, а начальный номер – 20, то последующим записям будут присвоены номера 25, 30, 35, 40 и т. д. 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 изменить нумерацию записей для указанного списка доступа в соответствии с начальным номером из параметра *STARTING-SEQUENCE-NUMBER* и шагом, заданным с помощью параметра *INCREMENT*.

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

После изменения начального порядкового номера или значения шага порядковые номера всех предыдущих правил (включая правила, назначенные пользователем) будут изменены согласно новым настройкам. Если сгенерированный порядковый номер превышает максимально допустимое значение, то существующая нумерация записей не изменится.

**Пример**

В примере ниже показано, как изменить нумерацию записей для списка доступа на основе IP-адресации 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 extended access-list R&D
Switch(config-ip-ext-acl)# 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 позволяет включить аппаратный счетчик ACL указанного списка управления доступом (access-list) для функций ограничения доступа (access group) или access map для фильтрации на основе VLAN. При использовании формы **no** команда отключит аппаратные счетчики для списков управления доступом.

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

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

**Параметры**

| | |
|---|---|
| **access-group** *ACCESS-LIST-NAME* | Имя конфигурируемого списка доступа. |
| **access-group** *ACCESS-LIST-NUMBER* | Номер конфигурируемого списка доступа. |
| **vlan-filter** *ACCESS-MAP-NAME* | Имя конфигурируемой access map. |

**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, к которым применимо каждое правило.

Команда с параметром **vlan-filter** включает аппаратный счетчик ACL для всех VLAN, к которым применяется определенная VLAN access map. Число пакетов, разрешенных каждой из access map, подсчитывается.

**Пример**

В данном примере показан процесс включения функции аппаратного счетчика ACL.

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

## *4.3. action*

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

**action {forward | drop | redirect** *INTERFACE-ID***}**

**no action**

**Параметры**

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

**По умолчанию**

По умолчанию производится действие **forward**.

**Режим ввода команды**

VLAN Access-map Sub-map Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

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

```
Switch# show vlan access-map
VLAN access-map vlan-map 20
  match mac address: ext_mac(ID: 6856)
  action: forward
Switch# configure terminal
```

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

## *4.4. clear acl-hardware-counter*

Данная команда используется для сброса аппаратных счетчиков ACL.

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

**Параметры**

| | |
|---|---|
| **access-group** *ACCESS-LIST-NAME* | Имя удаляемого списка доступа. |
| **access-group** *ACCESS-LIST-NUMBER* | Номер конфигурируемого списка доступа. |
| **vlan-filter** *ACCESS-MAP-NAME* | Имя удаляемой access map. |

**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). Если в параметре **vlan-filter** не указано имя access map, будут сброшены все аппаратные счетчики для фильтрации на основе VLAN.

**Пример**

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

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

## *4.5. expert access-group*

Данная команда используется для применения указанного списка управления доступом expert (expert ACL) к интерфейсу. При использовании формы **no** команда отменит применение.

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

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

**Параметры**

| | |
|---|---|
| *NAME* | Имя настраиваемого списка управления доступом expert |

| | |
|---|---|
| | (expert access-list). Максимальное число допустимых символов в имени – 32. |
| *NUMBER* | Номер настраиваемого списка управления доступом expert (expert access-list). |
| **in** | (Опционально) Фильтрация входящих пакетов на интерфейс. Если направление не указано, используется значение **in**. |
| **out** | (Опционально) Фильтрация исходящих пакетов для передачи интерфейсу. |

**По умолчанию**

Нет.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

В данном примере показан процесс применения списка 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
eth1/0/2:
  Inbound expert access-list : exp_acl(ID: 8999)
Switch#
```

## *4.6. expert access-list*

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

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

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

**Параметры**

| | |
|---|---|
| *NAME* | Имя конфигурируемого расширенного списка доступа expert. Максимальное число допустимых символов в имени – 32. |

| | |
|---|---|
| *NUMBER* | Идентификационный номер (ID number) экспертного списка доступа. Для расширенных списков доступа expert допустимо значение от 8000 до 9999. |

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

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

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

Total Entries: 1

Switch#
```

## *4.7. ip access-group*

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

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

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

**Параметры**

| | |
|---|---|
| *NAME* | Имя используемого списка доступа IP. Максимальное число допустимых символов в имени – 32. |
| *NUMBER* | 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 **in**. |
| **out** | (Опционально) Указывает, что список доступа IP будет применен для проверки пакетов в исходящем направлении. |

**По умолчанию**

Нет.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

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

**Пример**

В данном примере показан процесс настройки списка доступа IP «Strict-Control» в качестве группы доступа IP для порта Ethernet 6/0/2.

```
Switch# configure terminal
Switch(config)# interface eth6/0/2
Switch(config-if-gi)#ip access-group Strict-Control
The remaining applicable IP related access entries are 2500
The remaining applicable port operators are 10
Switch(config-if-gi)#
```

## *4.8. ip access-list*

Данная команда используется для создания или изменения списка доступа IP (IP access list). При использовании команды произойдет вход в режим IP Access List Configuration Mode. При использовании формы **no** команда удалит список доступа IP.

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

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

**Параметры**

| | |
|---|---|
| **extended** | (Опционально) Указывает, что список доступа IP является расширенным списком доступа IP (extended IP access list), и есть возможность применить больше опций фильтрации. Если параметр не указан, список доступа будет считаться стандартным. |
| *NAME* | Назначаемое имя списка доступа IP. Максимальное число допустимых символов в имени – 32. Первым символом должна быть буква. |
| *NUMBER* | 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**

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

**Пример**

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

```
Switch# configure terminal
Switch(config)# ip access-list extended Strict-Control
Switch(config-ip-ext-acl)# permit tcp any 10.20.0.0 255.255.0.0
Switch(config-ip-ext-acl)# exit
Switch(config)# ip access-list pim-srcfilter
Switch(config-ip-acl)# permit host 172.16.65.193 any
Switch(config-ip-acl)#
```

## *4.9. ipv6 access-group*

Данная команда используется для назначения списка доступа IPv6 (IPv6 access list), который будет применяться к интерфейсу. При использовании формы **no** команда удалит список доступа IPv6.

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

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

**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 **in**. |
| **out** | (Опционально) Указывает, что список доступа IPv6 будет применен для проверки пакетов в исходящем направлении. |

**По умолчанию**

Нет.

**Режим ввода команды.**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

К одному и тому же интерфейсу нельзя применить несколько списков доступа одинакового типа, при этом могут применяться списки доступа разных типов. Привязка группы доступа (access

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

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

**Пример**

В данном примере показано, как применить список доступа IPv6 «ip6-control» в качестве группы доступа IP для 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 2500
The remaining applicable port operators are 10
Switch(config-if)#
```

## *4.10. ipv6 access-list*

Данная команда используется для создания или изменения списка доступа IPv6. При использовании команды произойдет вход в режим IPv6 Access List Configuration Mode. При использовании формы **no** команда удалит список доступа IPv6.

**ipv6 access-list [extended]** *NAME* **[***NUMBER***]**

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

**Параметры**

| | |
|---|---|
| *NAME* | Назначаемое имя списка доступа IPv6. Максимальное число допустимых символов в имени – 32. |
| *NUMBER* | (Опционально) Номер ID (ID number) списка доступа IPv6. Для стандартных списков доступа IPv6 диапазон значений от 11000 до 12999. Для расширенных списков доступа IPv6 доступен диапазон значений от 13000 до 14999. |
| **extended** | (Опционально) Указывает, что список доступа IPv6 является расширенным списком доступа IPv6, и есть возможность применить больше опций фильтрации.<br>Если параметр не указан, список доступа IPv6 будет считаться стандартным. |

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

В данном примере показано, как настроить расширенный список доступа IPv6 с именем «ip6-control».

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

В данном примере показано, как настроить стандартный список доступа IPv6 с именем «ip6-std-control».

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

## *4.11. list-remark*

Данная команда используется для добавления комментариев к указанным спискам ACL. При использовании формы **no** команда удалит комментарии.

**list-remark** *TEXT*

**no list-remark**

**Параметры**

| | |
|---|---|
| *TEXT* | Текст комментария (не более 256 символов). |

**По умолчанию**

Нет.

**Режим ввода команды**

Access-list Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

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

Switch#
```

## *4.12. mac access-group*

Данная команда используется для назначения списка управления доступом на базе MAC-адресации (MAC access list), который будет применяться к интерфейсу. При использовании формы **no** команда удалит группу доступа с интерфейса.

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

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

**Параметры**

| | |
|---|---|
| *NAME* | Укажите имя используемого списка доступа на основе MAC. |
| *NUMBER* | Укажите номер используемого списка управления доступом на основе MAC. |
| **in** | (Опционально) Указывает, что список доступа на основе MAC будет применен для проверки пакетов во входящем направлении. Если параметр не указан, используется значение **in**. |
| **out** | (Опционально) Указывает, что список доступа на основе MAC будет применен для проверки пакетов в исходящем направлении. |

**По умолчанию**

Нет.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

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

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

**Пример**

В данном примере показано, как применить список доступа на основе MAC «daily-profile» к Ethernet 5/0/1.

```
Switch# configure terminal
Switch(config)# interface eth5/0/1
Switch(config-if-gi)# mac access-group daily-profile in
The remaining applicable MAC access entries are 204
Switch(config-if-gi)#
```

## *4.13. mac access-list*

Данная команда используется для создания или изменения списков управления доступом на базе MAC-адресации. Команда позволяет войти в режим MAC Access List Configuration Mode. При использовании формы **no** команда удалит список управления доступом MAC.

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

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

**Параметры**

| | |
|---|---|
| *NAME* | Укажите имя списка управления доступом MAC (MAC access list). Максимально допустимая длина – 32 символа. |
| *NUMBER* | Укажите номер ID (ID number) списка управления доступом на основе MAC. Для расширенных списков доступа MAC доступно значение 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 правила. Указанное имя должно быть уникальным среди всех списков доступа. Имя чувствительно к регистру. Если номер списка доступа не задан, автоматически будет назначен самый большой неиспользуемый номер из диапазона номеров списков доступа на основе MAC.

**Пример**

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

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

## *4.14. match ip address*

Данная команда используется для сопоставления списка доступа IP с настраиваемой sub-map. При использовании формы **no** команда удалит совпадающую запись.

**match ip address {***ACL-NAME* **|** *ACL-NUMBER***}**

**no match ip address**

**Параметры**

| | |
|---|---|
| *ACL-NAME* | Укажите имя списка управления доступом (ACL access list). Максимально допустимая длина – 32 символа. |
| *ACL-NUMBER* | Укажите номер списка управления доступом IP (IP ACL). |

**По умолчанию**

Нет.

**Режим ввода команды**

VLAN Access-map Sub-map Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте данную команду, чтобы сопоставить список доступа IP с настроенной sub-map. С одной sub-map может быть сопоставлен только один список доступа (IP access list, IPv6 access list или MAC access list). IP Sub-map проверяет только IP-пакеты. При вводе новой команды предыдущие настройки будут перезаписаны.

**Пример**

В данном примере показано, как настроить сопоставление содержимого с sub-map.

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

VLAN access-map vlan-map 20
  match ip address:  sp1(ID: 1999)
  action: forward

Switch#
```

## *4.15. match ipv6 address*

Данная команда используется для сопоставления списков доступа IPv6 с настраиваемыми sub-maps. При использовании формы **no** команда удалит соответствующую запись.

**match ipv6 address {***ACL-NAME* **|** *ACL-NUMBER***}**

**no match ipv6 address**

**Параметры**

| | |
|---|---|
| *ACL-NAME* | Укажите имя списка управления доступом IPv6 (IPv6 ACL). Максимально допустимая длина – 32 символа. |
| *ACL-NUMBER* | Укажите номер списка управления доступом IPv6 (IPv6 ACL). |

**По умолчанию**

Нет.

**Режим ввода команды**

VLAN Access-map Sub-map Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте данную команду, чтобы сопоставить список доступа IPv6 с настроенной sub-map. С одной sub-map может быть сопоставлен только один список доступа (IP access list, IPv6 access list или MAC access list). IPv6 sub-map проверяет только IPv6-пакеты. При вводе новой команды предыдущие настройки будут перезаписаны.

**Пример**

В данном примере показано, как настроить сопоставление содержимого с sub-map.

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

VLAN access-map vlan-map 20
  match ipv6 address:  sp1(ID: 12999)
  action: forward

Switch#
```

## *4.16. match mac address*

Данная команда используется для сопоставления списков доступа MAC (MAC access lists) с настраиваемыми sub-maps. При использовании формы **no** команда удалит соответствующую запись.

**match mac address {***ACL-NAME* **|** *ACL-NUMBER***}**

**no match mac address**

**Параметры**

| | |
|---|---|
| *ACL-NAME* | Укажите имя списка управления доступом MAC (ACL MAC). Максимально допустимая длина – 32 символа. |
| *ACL-NUMBER* | Укажите номер списка управления доступом MAC. |

**По умолчанию**

Нет.

**Режим ввода команды**

VLAN Access-map Sub-map Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте данную команду, чтобы сопоставить список доступа MAC (MAC access list) с настраиваемой sub-map. С одной sub-map может быть сопоставлен только один список доступа (IP access list, IPv6 access list или MAC access list). MAC Sub-map не проверяет IP-пакеты. При вводе новой команды предыдущие настройки будут перезаписаны.

**Пример**

В данном примере показано, как настроить сопоставление содержимого с sub-map.

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

VLAN access-map vlan-map 20
  match ip address:  sp1(ID: 3999)
  action: forward
```

```
VLAN access-map vlan-map 30
  match mac address:  ext_mac(ID: 7999)
  action: forward

Switch#
```

### *4.17. permit | deny (expert access-list)*

Данная команда используется для создания разрешающих или запрещающих правил фильтрации в списке ACL. При использовании формы **no** команда удалит запись.

**Расширенный список управления доступом Expert (Extended Expert ACL):**

**[***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** *OUTER-COS* **[inner** *INNER-COS***]] [{vlan** *OUTER-VLAN***} [inner** *INNER-VLAN***]] [fragments] [[precedence** *PRECEDENCE***] [tos** *TOS***] | dscp** *DSCP***] [time-range** *PROFILE-NAME***]**

**[***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* **[inner** *INNER-COS***]] [vlan** *OUTER-VLAN* **[inner** *INNER-VLAN***]] [[precedence** *PRECEDENCE***] [tos** *TOS***] | dscp** *DSCP***] [time-range** *PROFILE-NAME***]**

**[***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* **[inner** *INNER-COS***]] [vlan** *OUTER-VLAN* **[inner** *INNER-VLAN***]] [[precedence** *PRECEDENCE***] [tos** *TOS***] | dscp** *DSCP***] [time-range** *PROFILE-NAME***]**

**[***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* **[inner** *INNER-COS***]] [vlan** *OUTER-VLAN* **[inner** *INNER-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. |
| **inner** *INNER-COS* | (Опционально) Укажите значение внутреннего приоритета (inner priority). Доступен диапазон значений от 0 до 7. |
| **vlan** *OUTER-VLAN* | (Опционально) Укажите outer VLAN ID. |
| **inner** *INNER-VLAN* | (Опционально) Укажите inner VLAN ID. |
| **Any** | Укажите для использования любого MAC-адреса источника, любого MAC-адреса назначения, любого IP-адреса источника или |

| | |
|---|---|
| | любого IP-адреса назначения. |
| **host** *SRC-MAC-ADDR* | Укажите определенный MAC-адрес узла источника. |
| *SRC-MAC-ADDR SRC-MAC-WILDCARD* | Укажите группу MAC-адресов источника, используя значение битовой маски (wildcard). Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться. |
| **host** *DST-MAC-ADDR* | Укажите определенный MAC-адрес узла назначения. |
| *DST-MAC-ADDR DST-MAC-WILDCARD* | Укажите группу MAC-адресов назначения, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться. |
| **host** *SRC-IP-ADDR* | Укажите определенный IP-адрес узла источника. |
| *SRC-IP-ADDR SRC-IP-WILDCARD* | Укажите группу IP-адресов источника, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться. |
| **host** *DST-IP-ADDR* | Укажите определенный IP-адрес узла назначения. |
| *DST-IP-ADDR DST-IP-WILDCARD* | Укажите группу IP-адресов назначения, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться. |
| *PROTOCOL* | (Опционально) Укажите ID IP-протокола. |
| **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 значений от 0 до 63 или выбор из следующих имен DSCP: af11 - 001010, af12 - 001100, af13 -001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 - 110000, cs7 - 111000, default (по умолчанию) - 000000, ef - 101110. |
| **lt** *PORT* | (Опционально) Укажите для сопоставления, если значение порта меньше указанного. |
| **gt** *PORT* | (Опционально) Укажите для сопоставления, если значение порта больше указанного. |
| **eq** *PORT* | (Опционально) Укажите для сопоставления, если значение порта равно указанному. |
| **neq** *PORT* | (Опционально) Укажите для сопоставления, если значение порта не равно указанному. |

| | |
|---|---|
| **range** *MIN-PORT MAX-PORT* | (Опционально) Укажите для сопоставления, если значение попадает в указанный диапазон портов. |
| *TCP-FLAG* | (Опционально) Укажите поля TCP flag и указанные биты заголовка TCP с именем **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize) или **urg** (urgent). |
| **fragments** | (Опционально) Укажите для фильтрации фрагментов пакета. |
| **time-range** *PROFILE-NAME* | (Опционально) Укажите имя профиля временного интервала, связанного со списком доступа и определяющего 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 |

**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. Первой записи в списке присваивается начальный порядковый номер 10, а каждая новая запись получает последующий номер с шагом 10 (т. е. 20, 30, 40 и т.д.) и помещается в конец списка.

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

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

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

Даже если из команды **permit | deny (expert access-list)** удалить параметр **fragment** для параметров **tcp, udp** или **icmp**, пользователь все равно может использовать опцию *PROTOCOL* в команде **permit | deny (expert access-list)** для настройки параметра **fragment**.

**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)# deny tcp host 192.168.4.12 host 0013.0049.8272 any any
Switch(config-exp-nacl)# end
Switch# show access-lists

Extended Expert access list exp_acl(ID: 9999)
  10 deny tcp host 192.168.4.12 host 0013.0049.8272 any any

Switch#
```

## *4.18. permit | deny (ip access-list)*

Данная команда используется для добавления записи permit или deny. При использовании формы **no** команда удалит запись.

**Расширенный список управления доступом (Extended Access List):**

**[***SEQUENCE-NUMBER***] {permit | deny} tcp {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT***] {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***]**

**[***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***]**

**[***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***]**

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

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

**Стандартный список доступа IP** (Standard IP Access List):

**[***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***]**

**no** *SEQUENCE-NUMBER*

**Параметры**

| | |
|---|---|
| *SEQUENCE-NUMBER* | Укажите порядковый номер. Доступен диапазон от 1 до 65535. Чем меньше номер, тем выше приоритет правила permit/deny. |
| **any** | Укажите для использования любого IP-адреса источника или IP-адреса назначения. |

| | |
|---|---|
| **host** *SRC-IP-ADDR* | Укажите определенный IP-адрес узла источника. |
| *SRC-IP-ADDR* *SRC-IP-WILDCARD* | Укажите группу IP-адресов источника, используя значение битовой маски (wildcard). Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться. |
| **host** *DST-IP-ADDR* | Укажите определенный IP-адрес узла назначения. |
| *DST-IP-ADDR* *DST-IP-WILDCARD* | Укажите группу IP-адресов назначения, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться. |
| **precedence** *PRECEDENCE* | (Опционально) Укажите, чтобы пакеты могли фильтроваться по уровню приоритета (precedence). Доступны значения от 0 до 7. |
| **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. |
| **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 порта меньше указанного. |
| **gt** *PORT* | (Опционально) Укажите для сопоставления, если значение порта больше указанного. |
| **eq** *PORT* | (Опционально) Укажите для сопоставления, если значение порта равно указанному. |
| **neq** *PORT* | (Опционально) Укажите для сопоставления, если значение порта не равно указанному. |
| **range** *MIN-PORT MAX-PORT* | (Опционально) Укажите для сопоставления, если значение попадает в указанный диапазон портов. |
| **time-range** *PROFILE-NAME* | (Опционально) Укажите имя профиля временного интервала time-range, связанного со списком доступа и определяющего период его активации. |
| *TCP-FLAG* | (Опционально) Укажите поля TCP flag и указанные биты заголовка TCP с именем **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize) или **urg** (urgent). |
| **tcp, udp, igmp, ipinip, gre, esp, eigrp, ospf, pcp, pim, vrrp** | Укажите протоколы 4 уровня. |
| *PROTOCOL-ID* | (Опционально) Укажите Protocol ID. Доступен диапазон значений от 0 до 255. |
| *ICMP-TYPE* | (Опционально) Укажите тип сообщения ICMP. Доступны номера для типа сообщений от 0 до 255. |

| | |
|---|---|
| *ICMP-CODE* | (Опционально) Укажите код сообщения ICMP. Доступны номера для кода сообщений от 0 до 255. |
| *ICMP-MESSAGE* | (Опционально) Укажите сообщение ICMP. Для выбора доступны следующие предустановленные параметры:<br>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. Первой записи в списке присваивается начальный порядковый номер 10, а каждая новая запись получает последующий номер с шагом 10 (т. е. 20, 30, 40 и т.д.) и помещается в конец списка.

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

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

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

При создании правила сопоставления для стандартного списка доступа IP (IP standard access list) указываются 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 для сети 10.20.0.0, разрешить TCP-пакеты для узла 10.100.1.2, разрешить все TCP-пакеты для порта назначения TCP 80 и разрешить все ICMP-пакеты.

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

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

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

## *4.19. permit | deny (ipv6 access-list)*

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

**Расширенный список доступа IPv6 (Extended IPv6 Access List):**

**[***SEQUENCE-NUMBER***] {permit | deny} tcp {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDR/PREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT***] {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***]**

**[***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***]**

**[***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***]**

**[***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***]**

**[***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):**

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

**no** *SEQUENCE-NUMBER*

**Параметры**

| | |
|---|---|
| *SEQUENCE-NUMBER* | Укажите порядковый номер. Доступен диапазон от 1 до 65535. Чем меньше номер, тем выше приоритет правила permit/deny. |
| **any** | Укажите для использования любого IPv6-адреса источника или IPv6-адреса назначения. |

| | |
|---|---|
| **host** *SRC-IPv6-ADDR* | Укажите определенный IPv6-адрес узла источника. |
| *SRC-IPV6-ADDR/PREFIX-LENGTH* | Укажите сеть IPv6 источника. |
| **host** *DST-IPV6-ADDR* | Укажите определенный IPv6-адрес узла назначения. |
| *DST-IPV6-ADDR/PREFIX-LENGTH* | Укажите сеть IPv6 назначения. |
| **tcp, udp, icmp, esp, pcp ,sctp** | Укажите тип протокола 4 уровня. |
| **dscp** *VALUE* | (Опционально) Укажите совпадающее значение класса трафика в IPv6-хедере. Доступен диапазон от 0 до 63 или следующие DSCP-имена: af11 - 001010, af12 -001100, af13 - 001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 - 110000, cs7 - 111000, default (по умолчанию) - 000000, ef - 101110. |
| **lt** *PORT* | (Опционально) Укажите для сопоставления, если значение порта меньше указанного. |
| **gt** *PORT* | (Опционально) Укажите для сопоставления, если значение порта больше указанного. |
| **eq** *PORT* | (Опционально) Укажите для сопоставления, если значение порта равно указанному. |
| **neq** *PORT* | (Опционально) Укажите для сопоставления, если значение порта не равно указанному. |
| **range** *MIN-PORT MAX-PORT* | (Опционально) Укажите для сопоставления, если значение попадает в указанный диапазон портов. |
| *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 временного интервала, связанного со списком доступа и определяющего 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. Первой записи в списке присваивается начальный порядковый номер 10, а каждая новая запись получает последующий номер с шагом 10 (т. е. 20, 30, 40 и т.д.) и помещается в конец списка.

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

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

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

**Пример**

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

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

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

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

## *4.20. permit | deny (mac access-list)*

Данная команда используется для назначения правила, которое будет разрешать или запрещать продвижение пакетов. При использовании формы **no** команда удалит запись.

**[***SEQUENCE-NUMBER***] {permit | deny} {any | host** *SRC-MAC-ADDR* **|** *SRC-MAC-ADDR SRC-MAC-WILDCARD***} {any | host** *DST-MAC-ADDR* **|** *DST-MAC-ADDR DST-MAC-WILDCARD***} [ethernet-type** *TYPE MASK* **[cos** *VALUE* **[inner** *INNER-COS***]] [vlan** *VLAN-ID* **[inner** *INNER-VLAN***]] [time-range** *PROFILE-NAME***]**

**no** *SEQUENCE-NUMBER*

**Параметры**

| | |
|---|---|
| *SEQUENCE-NUMBER* | Укажите порядковый номер. Доступен диапазон от 1 до 65 535. Чем меньше номер, тем выше приоритет правила permit/deny. |
| **any** | Укажите для использования любого MAC-адреса источника или MAC-адреса назначения. |
| **host** *SRC-MAC-ADDR* | Укажите определенный MAC-адрес узла источника. |
| *SRC-MAC-ADDR SRC-MAC-WILDCARD* | Укажите группу MAC-адресов источника, используя значение битовой маски (wildcard). Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться. |
| **host** *DST-MAC-ADDR* | Укажите определенный MAC-адрес узла назначения. |
| *DST-MAC-ADDR DST-MAC-WILDCARD* | Укажите группу MAC-адресов назначения, используя значение битовой маски (wildcard). Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться. |
| **ethernet-type** *TYPE MASK* | (Опционально) Укажите Ethernet-тип фильтруемых пакетов в виде шестнадцатеричного числа с диапазоном значений от 0 до FFFF или используйте имя типа Ethernet. Доступны следующие имена: aarp, appletalk, decnet-iv, etype-6000, etype-8042, lat, lavc-sca, mop-console, mop-dump, vines-echo, vines-ip, xns-idp или arp. |
| **cos** *VALUE* | (Опционально) Укажите значение priority (приоритета) от 0 до 7. |
| **inner** *INNER-COS* | (Опционально) Укажите inner priority. Доступен диапазон от 0 до 7. |
| **vlan** *VLAN-ID* | (Опционально) Укажите VLAN-ID. |
| **inner** *INNER-VLAN* | (Опционально) Укажите Inner VLAN ID. |
| **time-range** *PROFILE-NAME* | (Опционально) Укажите имя профиля временного интервала, связанного со списком доступа и определяющего период его активации. |

**По умолчанию**

Нет.

**Режим ввода команды**

MAC Access-list Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

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

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

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

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

**Пример**

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

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

## *4.21. show access-group*

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

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

**Параметры**

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

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

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

**Пример**

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

```
Switch# show access-group

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

Switch#
```

## *4.22. show access-list*

Данная команда используется для просмотра информации о настройках списка доступа.

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

**Параметры**

| | |
|---|---|
| **ip** | (Опционально) Укажите для отображения всех списков доступа IP. |
| **mac** | (Опционально) Укажите для отображения всех списков доступа MAC. |
| **ipv6** | (Опционально) Укажите для отображения всех списков доступа IPv6. |
| **expert** | (Опционально) Укажите для отображения всех списков доступа Expert. |
| *NAME* **|** *NUMBER* | (Опционально) Укажите для отображения конкретного списка доступа. |
| **arp** | (Опционально) Укажите для отображения всех списков доступа ARP. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Команда отображает информацию о списках доступа. Если не указана конкретная опция, отображается перечень всех настроенных списков доступа. Если указан тип списка доступа, отображается детальная информация о соответствующем ему списке доступа. Если включен аппаратный счетчик ACL (ACL hardware counter) для списка доступа (access list) счетчик будет отображен на основе каждой записи списка доступа.

**Пример**

В данном примере показано, как 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 примере ниже 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)

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  Egr: 85201 packets)
20 permit tcp any host 10.100.1.2   (Ing: 6532 packets  Egr: 0 packets)
30 permit icmp any any   (Ing: 8758 packets  Egr: 4214 packets)

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

Switch#
```

## *4.23. show vlan access-map*

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

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

**Параметры**

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

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

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

**Пример**

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

```
Switch# show vlan access-map

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

Switch#
```

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

```
Switch# show vlan access-map

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

Switch#
```

## *4.24. show vlan filter*

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

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

**Параметры**

| | |
|---|---|
| **access-map** *MAP-NAME* | (Опционально) Укажите имя VLAN access-map. Имя не может |

| | |
|---|---|
| | содержать более 32 символов. |
| **vlan** *VLAN-ID* | (Опционально) Укажите VLAN ID. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

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

**Пример**

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

```
Switch# show vlan filter

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

Switch#

Switch# show vlan filter vlan 5

VLAN ID 5
  VLAN Access Map: aa

Switch#
```

## *4.25. vlan access-map*

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

**vlan access-map** *MAP-NAME* **[***SEQUENCE-NUM***]**

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

**Параметры**

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

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

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

К пакету, совпадающему с sub-map (т. е. пакет разрешен соответствующим списком доступа), применяется действие, определенное для данной sub-map. Проверка остальных sub-maps проводиться не будет. Если пакет не соответствует текущей sub-map, проверяться будет следующая sub-map.

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

**Пример**

В данном примере показано, как создать VLAN access map.

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

## *4.26. vlan filter*

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

**vlan filter** *MAP-NAME* **vlan-list** *VLAN-ID-LIST*

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

**Параметры**

| | |
|---|---|
| *MAP-NAME* | Укажите имя VLAN access map. |
| **vlan-list** *VLAN-ID-LIST* | Укажите список VLAN ID. |

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

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

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

VLAN Map vlan-map
  Configured on VLANs: 5

Switch#
```

# 5. Команды управления доступом

## *5.1. access class*

Данная команда позволяет задать список, которому необходимо ограничить доступ к управлению устройством. Используйте форму **no**, чтобы отменить проверку указанного списка доступа.

**access-class** *IP-ACL*

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

**Параметры**

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

**По умолчанию**

Нет.

**Режим ввода команды**

Line Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Команда позволяет задать списки, которым необходимо ограничить доступ к сессии. Максимальное число списков доступа - 2. Если два списка доступа уже применены, попытка применить новый список доступа отклоняется до тех пор, пока один из примененных списков не будет удален с помощью формы **no.**

**Пример**

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

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

## *5.2. banner login*

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

**banner login** *cMESSAGEc*

**no banner login**

**Параметры**

| | |
|---|---|
| *c* | Разделитель текста баннера приветствия, например, знак решетки (#). В тексте баннера приветствия употребление символа разделителя недопустимо. |

| | |
|---|---|
| *MESSAGE* | Текст баннера приветствия, отображаемый до появления приглашения на ввод имени пользователя и пароля. |

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда позволяет настроить баннер-сообщение, которое будет отображаться после успешного входа пользователя в систему. После команды **banner login** введите как минимум один пробел и любой символ-разделитель на выбор. Далее введите одну или несколько строк текста, закончив сообщение вторым разделителем.

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

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

**Пример**

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

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

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

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

## *5.3. prompt*

Данная команда используется для изменения приглашения на ввод команды в командной строке CLI. При использовании формы **no** команда вернет настройки по умолчанию.

**prompt** *STRING*

**no prompt**

**Параметры**

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

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда позволяет настроить приглашение на ввод команды. Если в качестве приглашения выбрать зашифрованное имя сервера SNMP, то зашифрованы будут только первые 15 символов. Подсказка может отобразить только 15 символов. Символ уровня привилегий в приглашении будет отображаться последним.

Используются следующие обозначения:

> – для приглашения пользовательского режима;

# – для приглашения привилегированного режима.

**Пример**

В данном примере показано, как настроить новое приглашение «BRANCH A», используя учетную запись администратора.

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

## *5.4. enable password*

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

**enable password [level** *PRIVILEGE-LEVEL***] [0| 7]** *PASSWORD*

**no enable password [level** *PRIVILEGE-LEVEL***]**

**Параметры**

| | |
|---|---|
| **level** *PRIVILEGE-LEVEL* | Указывается уровень привилегий пользователя – от 1 до 15. Если данный параметр не указан, или используется форма no, уровень по умолчанию – 15. |
| **0** *PASSWORD* | Указывается пароль для доступа к коммутатору. Пароль может содержать пробелы. Чувствителен к регистру. Это опция по умолчанию. Максимальная длина незашифрованного пароля – 32 символа.<br>(Диапазон: 1 – 32) |
| **7** *PASSWORD* | Указывается зашифрованный пароль на основе SHA-1. Длина пароля ограничена 35 байтами. Пароль чувствителен к регистру и зашифрован. |

**По умолчанию**

По умолчанию пароль не задан. Данная строка остается пустой.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

В привилегированном режиме для входа на определенный уровень привилегий используется соответствующий данному уровню пароль. Каждый уровень имеет только один пароль.

**Пример**

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

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

## *5.5. ip http server*

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

**ip http server**

**no ip http server**

**Параметры**

Нет.

**По умолчанию**

По умолчанию данная опция отключена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

В данном примере показано, как включить сервер HTTP.

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

## *5.6. ip http secure-server*

Данная команда позволяет включить сервер HTTPS. При использовании команды **ip http secure-server ssl-service-policy** необходимо указать политику сервиса SSL для HTTPS. При использовании формы **no** команда отключит сервер HTTPS.

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

**no ip http secure-server**

**Параметры**

| | |
|---|---|
| **ssl-service-policy** *POLICY-NAME* | (Опционально) Имя политики сервиса SSL. Используйте параметр **ssl-service-policy,** только если вы уже указали политику сервиса SSL 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 12.

**Использование команды**

Данная команда позволяет включить сервер HTTPS и использовать встроенный локальный сертификат для HTTPS.

**Пример**

В данном примере показано, как включить HTTPS-сервер.

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

## *5.7. ip http access-class*

Данная команда позволяет назначить список, которому необходимо ограничить доступ к HTTP-серверу. Используйте форму **no**, чтобы отменить проверку указанного списка доступа.

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

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

**Параметры**

| | |
|---|---|
| *IP-ACL* | Указывается стандартный список доступа IP-адресов. Поле адреса источника в правиле определяет, является ли узел доверенным или нет. |

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

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

## *5.8. ip http service-port*

Данная команда позволяет указать порт для HTTP-соединения. При использовании формы **no** команда вернет настройки по умолчанию (порт 80).

**ip http service-port** *TCP-PORT*

**no ip http service-port**

**Параметры**

| | |
|---|---|
| *TCP-PORT* | Номер порта TCP. Диапазон портов TCP – от 1 до 65535. Как правило, для протокола HTTP назначается TCP-порт 80. |

**По умолчанию**

По умолчанию используется порт 80.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

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

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

## *5.9. ip http timeout-policy idle*

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

**ip http timeout-policy idle** *INT*

**no ip http timeout-policy idle**

**Параметры**

| | |
|---|---|
| *INT* | Значение таймера в секундах. Допустимый диапазон от 60 до 36000. |

**По умолчанию**

По умолчанию значение составляет 180 секунд.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

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

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

## *5.10. ip telnet server*

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

**ip telnet server**

**no ip telnet server**

**Параметры**

Нет.

**По умолчанию**

По умолчанию данная опция включена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

В данном примере показан процесс включения сервера Telnet.

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

## *5.11. ip telnet service port*

Данная команда позволяет задать порт, используемый Telnet-сервером. При использовании формы **no** команда вернет настройки по умолчанию.

**ip telnet service-port** *TCP-PORT*

**no ip telnet service-port**

**Параметры**

| | |
|---|---|
| *TCP-PORT* | Укажите номер TCP-порта. Доступен 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 по Telnet.

**Пример**

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

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

## *5.12. ip telnet source-interface*

Данная команда позволяет задать IP-адрес интерфейса, который будет использоваться в качестве адреса источника Telnet-пакетов при установке Telnet-соединения. При использовании формы **no** команда вернет настройки по умолчанию.

**ip telnet source-interface** *INTERFACE-ID*

**no ip telnet source-interface**

**Параметры**

| | |
|---|---|
| *INTERFACE-ID* | IP-адрес интерфейса, который будет использоваться в качестве адреса источника пакетов при установке Telnet-соединения. |

**По умолчанию**

По умолчанию используется IP-адрес ближайшего интерфейса.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда позволяет указать IP-адрес интерфейса, который будет использоваться в качестве адреса пакетов при установке Telnet-соединения.

**Пример**

В данном примере показан процесс настройки VLAN 100 в качестве исходного интерфейса для Telnet-пакетов для инициирования подключения по Telnet.

```
Switch# configure terminal
Switch(config)# ip telnet source-interface vlan100
Switch(config)#
```

## *5.13. line*

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

**line {console | telnet | ssh}**

**Параметры**

| | |
|---|---|
| **console** | Локальная консольная сессия терминала. |
| **telnet** | Сессия терминала Telnet. |
| **ssh** | Сессия терминала SSH. |

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда позволяет войти в режим Line Configuration Mode.

**Пример**

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

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

## *5.14. service password-recovery*

Данная команда позволяет включить функцию восстановления пароля. При использовании формы **no** команда отключит функцию восстановления пароля.

**service password-recovery**

**no service password-recovery**

**Параметры**

Нет.

**По умолчанию**

По умолчанию данная опция включена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Данная команда позволяет включить функцию восстановления пароля. Функция восстановления пароля включена по умолчанию.

**Пример**

В данном примере показан процесс отключения функции восстановления пароля.

```
Switch# configure terminal
Switch(config)# no service password-recovery
Switch(config)#
```

## *5.15. service password-encryption*

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

**service password-encryption [7 | 15]**

**no service password-encryption**

**Параметры**

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

**По умолчанию**

По умолчанию данная опция включена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

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

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

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

**Пример**

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

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

## *5.16. 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 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 показан процесс отображения информации о настройках терминала для текущей сессии.

```
Switch# show terminal

Terminal Settings:
Length: 24 lines
Width: 80 columns
Default Length: 24 lines
Default Width: 80 columns
Baud rate: 9600 bps

Switch#
```

## *5.17. show ip http server*

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

**show ip http server**

**Параметры**
Нет.

**По умолчанию**
Нет.

**Режим ввода команды**
User 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 показан процесс отображения информации о состоянии HTTP-сервера.

```
Switch# show ip http server

ip http server state :  enable

Switch#
```

## *5.18. show ip http secure-server*

Данная команда используется для отображения информации о состоянии SSL.

**show ip http secure-server**

**Параметры**
Нет.

**По умолчанию**
Нет.

**Режим ввода команды**
User EXEC Mode.
Любой режим конфигурирования.

**Уровень команды по умолчанию**
Уровень 1.

**Использование команды**
Данная команда используется для отображения информации о состоянии SSL.

**Пример**
В данном примере показан процесс отображения информации о состоянии SSL.

```
Switch# show ip http secure-server

ip http secure-server state :  disable

Switch#
```

## *5.19. show users*

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

**show users**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

UserEXEC 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 показан процесс отображения информации обо всех сессиях.

```
Switch# show users

ID   Type          User-Name           Privilege    Login-Time     IP address
--------------------------------------------------------------------------------
0   * console      admin               15           12M5S
1   telnet         monitoruser         2            3DT2H20M15S     172.171.160.100
10  SSH            123                 15           1M45S           172.171.160.100

Total Entries: 3

Switch#
```

## *5.20. telnet*

Данная команда позволяет подключиться к другому устройству с поддержкой Telnet.

**telnet [***IP-ADDRESS* | *IPV6-ADDRESS***] [***TCP-PORT***]**

**Параметры**

| | |
|---|---|
| *IP-ADDRESS* | IPv4-адрес узла. |
| *IPV6-ADDRESS* | IPv6-адрес узла. |
| *TCP-PORT* | Номер TCP-порта. Доступен диапазон портов TCP от 1 до 65535. Как правило, для Telnet назначается TCP-порт 23. |

**По умолчанию**

Нет.

**Режим ввода команды**

EXEC Mode.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная функция Telnet-клиента используется для связи с другим устройством с помощью Telnet.

Telnet поддерживает особые команды в виде Telnet-последовательностей, которые преобразуют стандартные функции управления терминалом в функции, специфические для системы. Для выполнения Telnet-команды введите последовательность escape, а затем символ команды. Последовательность escape по умолчанию CTRL+_ (нажмите и удерживайте CTRL, Shift и нижнее подчеркивание). Специфические команды Telnet будут отображаться следующим образом:

**e** - отключение от Telnet. Для отключения сессии Telnet может использоваться как прописная, так и строчная латинская буква "e".

Если нажать другую клавишу, терминал вернется к изначально активной сессии Telnet.

На коммутаторе может быть открыто несколько Telnet-сессий, и каждая открытая Telnet-сессия может поддерживать свое клиентское ПО Telnet-клиента одновременно.

**Пример**

В данном примере показан процесс подключения к IP-адресу 10.90.90.91 с помощью порта 23. IP-адрес 10.90.90.91 является интерфейсом управления DXS-3600-32S, позволяющим пользователю войти в учетную запись.

```
Switch# telnet 10.90.90.91

                    DXS-3600-32S Gigabit Ethernet Switch

                          Command Line Interface
                         Firmware: Build 2.40.041
          Copyright(C) 2015 D-Link Corporation. All rights reserved.

Password required, but none set

Switch#
```

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

```
Switch#telnet 10.90.90.91

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

Switch# telnet 10.90.90.91 3500

                      DXS-3600-32S Gigabit Ethernet Switch

                              Command Line Interface
                             Firmware: Build 2.40.041
           Copyright(C) 2015 D-Link Corporation. All rights reserved.

Password required, but none set

Switch#
```

## *5.21. terminal length*

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

**terminal length** *NUMBER*

**no terminal length**

**terminal length default** *NUMBER*

**no terminal length default**

**Параметры**

| | |
|---|---|
| *NUMBER* | 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**

User/Privileged EXEC Mode для команды **terminal length.**

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

**Уровень команды по умолчанию**

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

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

**Использование команды**

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

Если в команде **terminal length** указано значение, отличное от 0, например 50, то вывод приостанавливается после каждых 50 строк. Данная команда используется для настройки количества отображаемых строк во время текущей сессии. Команда также применяется для сессий Telnet и SSH. Доступны значения от 0 до 512. Значение по умолчанию – 24. При выборе 0 коммутатор будет автоматически выводить всю информацию без пауз.

Если вывод одной команды выходит за границы экрана, то такой вывод приостанавливается и в нижней части экрана появляется приглашение **-- More --.** При появлении приглашения --**More--** нажмите CTRL+C, q, Q или ESC, чтобы прервать вывод и вернуться к приглашению. Нажмите пробел для отображения дополнительного экрана вывода или нажмите Return для отображения еще одной строки вывода. При настройке длины экрана на 0 отключается функция прокручивания, из-за чего весь вывод экрана отображается сразу. Пока не будет использовано ключевое слово **default**, изменения значения terminal length будут применяться только к текущей сессии. При использовании формы **no** данной команды количество строк на экране терминала сбрасывается к 24.

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

**Пример**

В данном примере показан процесс изменения количества строк на 60.

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

## *5.22. terminal speed*

Данная команда используется для настройки скорости терминала. При использовании формы **no** команда вернет настройки по умолчанию.

**terminal speed** *BPS*

**no terminal speed**

**Параметры**

| | |
|---|---|
| *BPS* | Скорость консоли в бит/с. |

**По умолчанию**

Значение по умолчанию – 115200.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

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

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

## *5.23. session-timeout*

Данная команда позволяет задать значение тайм-аута сессии. При использовании формы **no** команда вернет настройки по умолчанию.

**session-timeout** *MINUTES*

**no session-timeout**

**Параметры**

| | |
|---|---|
| *MINUTES* | Таум-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, по истечении которого произойдет автоматический выход из учетной записи.

**Пример**

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

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

## *5.24. terminal width*

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

**terminal width** *NUMBER*

**no terminal width**

**terminal width default** *NUMBER*

**no terminal width default**

**Параметры**

| | |
|---|---|
| *NUMBER* | Количество символов, отображаемых на экране. Допустимы значения от 40 до 255. |

**По умолчанию**

Значение по умолчанию – 80.

**Режим ввода команды**

User/Privileged EXEC Mode для команды **terminal width.**

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

**Уровень команды по умолчанию**

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

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

**Использование команды**

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

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

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

**Пример**

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

```
Switch# show terminal

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

Switch# terminal width 120
Switch# show terminal

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

Switch #
```

## *5.25. username*

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

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

**no username [***NAME***]**

**Параметры**

| | |
|---|---|
| *NAME* | Имя пользователя (не более 32 символов). |
| **privilege** *LEVEL* | (Опционально) Уровень привилегий для каждого пользователя. Диапазон доступных уровней: от 1 до 15. |

| | |
|---|---|
| **nopassword** | (Опционально) Указывает, что для данной учетной записи не будет применяться пароль. |
| **password** | (Опционально) Указывает, что для данной учетной записи будет применяться пароль. |
| **0** | (Опционально) Пароль в обычном текстовом виде. Длина пароля может составлять от 1 до 32 символов и содержать пробелы. Пароль чувствителен к регистру. Если синтаксис пароля не указан, используется обычный текст. |
| **7** | (Опционально) Пароль, зашифрованный на основе SHA-1. Длина пароля ограничена 35 байтами. Пароль чувствителен к регистру. Пароль зашифрован. Если синтаксис пароля не указан, используется обычный текст. |
| **15** | (Опционально) Пароль, зашифрованный на основе MD5. Длина пароля ограничена 31 байтом. Пароль чувствителен к регистру. Пароль зашифрован. Если синтаксис пароля не указан, используется обычный текст. |
| *PASSWORD* | (Опционально) Пароль на основе одного из указанных выше параметров. |

**По умолчанию**

По умолчанию используется система аутентификации без учетной записи.

Если не указано другое, используйте 1.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Данная команда позволяет создать учетную запись пользователя с различными уровнями доступа. Если пользователь входит в систему с уровнем привилегий 1, он попадает в режим User EXEC Mode. Для перехода в режим Privileged EXEC Mode ему необходимо использовать команду **enable**.

Если пользователь входит с уровнем привилегий 2 или выше, он сразу попадает в режим Privileged EXEC Mode. Данный режим доступен уровням 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. После этого пользователь может перейти в режим Privileged EXEC Mode с помощью команды **enable**.

**Пример**

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

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

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

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

## *5.26. password*

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

**password [0 | 7 | 15]** *PASSWORD*

**no password**

**Параметры**

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

**По умолчанию**

Нет.

**Режим ввода команды**

Line Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

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

**Пример**

В данном примере показан процесс создания пароля для сессии консоли.

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

## *5.27. clear line*

Данная команда используется для завершения сессии подключения.

**clear line** *LINE-ID*

**Параметры**

| | |
|---|---|
| *LINE-ID* | line ID сессии соединения, который необходимо отключить. |

**По умолчанию**

Нет.

**Режим ввода команды**

Privileged EXEC Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Данная команда позволяет отключить активную сессию коммутатора. Идентификатор (Line ID) присваивается при создании сессии подключения. Используйте команду **show users** для просмотра активных сессий.

Данная команда может отключить только сессии SSH и Telnet.

**Пример**

В данном примере показан процесс отключения сессии 1.

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

# 6. Команды предотвращения атак ARP Spoofing

## *6.1. ip arp spoofing-prevention*

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

**ip arp spoofing-prevention** *GATEWAY-IP GATEWAY-MAC* **interface** *INTERFACE-ID* **[, | -]**

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

**Параметры**

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

**По умолчанию**

По умолчанию записей нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

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

Указать можно только физические порты.

**Пример**

В данном примере показан процесс настройки записи ARP Spoofing Prevention с IP-адресом 10.254.254.251 и MAC-адресом 00-00-00-11-11-11 для Ethernet-порта 1/0/1.

```
Switch#configure terminal
Switch(config)# ip arp spoofing-prevention 10.254.254.251 00-00-00-11-11-11 interface
ethernet 1/0/10
Switch(config)#
```

## *6.2. show ip arp spoofing-prevention*

Данная команда используется для отображения настроек ARP Spoofing Prevention.

**show ip arp spoofing-prevention**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для отображения всех записей ARP Spoofing Prevention.

**Пример**

В данном примере показано, как включить отображение всех записей ARP Spoofing Prevention.

```
Switch# show ip arp spoofing-prevention

IP              MAC               Interfaces
--------------- ----------------- --------------------------
10.254.254.251  00-00-00-11-11-11 ethernet 1/0/10

Total Entries: 1

Switch#
```

**Отображаемые параметры**

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

# 7. Команды Authentication, Authorization и Accounting (AAA)

## *7.1. aaa accounting commands*

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

**aaa accounting commands** *LEVEL* **{default |** *LIST-NAME***} start-stop** *METHOD1* **[***METHOD2***...]**

**no aaa accounting commands** *LEVEL* **{default |** *LIST-NAME***}**

**Параметры**

| | |
|---|---|
| *LEVEL* | Укажите уровень привилегий, на котором необходимо активировать аккаунтинг для всех команд **configure**. Допустимые уровни привилегий: от 1 до 15. |
| **default** | Указывается для использования списка методов аккаунтинга по умолчанию. |
| *LIST-NAME* | Укажите имя списка методов (не более 32 символов). |
| *METHOD1* **[***METHOD2***...]** | Укажите список методов, который необходимо выполнить алгоритму аккаунтинга в заданной последовательности. Введите от одного до четырех методов. Для установки метода используйте ключевые слова.<br>**group tacacs+** – используются серверы, определенные командой **TACACS+ server host**.<br>**group** *GROUP-NAME* – используются группы серверов, определенных командой **aaa group server tacacs+**.<br>**none** – аккаунтинг не выполняется. |

**По умолчанию**

Метод аккаунтинга AAA не настроен.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Используйте данную команду для настройки списка методов аккаунтинга команд**.**

**Пример**

В данном примере показано, как создать список методов аккаунтинга для уровня привилегий 15, используя TACACS+, который будет отправлять accounting-сообщения, когда пользователь входит и выходит из системы.

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

## *7.2. aaa accounting exec*

Данная команда используется для настройки списка методов, используемого для аккаунтинга сессий EXEC для конкретного терминала. Используйте форму **no** для отключения аккаунтинга EXEC.

**aaa accounting exec {default |** *LIST-NAME***} start-stop** *METHOD1* **[***METHOD2***...]**

**no aaa accounting exec {default |** *LIST-NAME***}**

**Параметры**

| | |
|---|---|
| **default** | Указывается для использования списка методов аккаунтинга EXEC по умолчанию. |
| *LIST-NAME* | Укажите имя списка методов (не более 32 символов). |
| *METHOD1* **[***METHOD2***...]** | Укажите список методов, который необходимо выполнить алгоритму аккаунтинга в заданной последовательности. Введите от одного до четырех методов. Для установки метода используйте ключевые слова.<br>**group radius** – используются серверы, определенные командой RADIUS server host.<br>**group tacacs+** – используются серверы, определенные командой TACACS+ server host.<br>**group** *GROUP-NAME* – используются группы серверов, определенные командой AAA group server.<br>**none** – аккаунтинг не выполняется. |

**По умолчанию**

Метод аккаунтинга AAA не настроен.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Используйте данную команду для настройки списка методов аккаунтинга сессий EXEC.

**Пример**

В данном примере показано, как создать список методов для аккаунтинга действий пользователей, используя RADIUS, который будет отправлять accounting-сообщения, когда пользователь входит и выходит из системы.

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

## *7.3. aaa accounting network*

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

**aaa accounting network default start-stop** *METHOD1* **[***METHOD2***...]**

**no aaa accounting network default**

**Параметры**

| | |
|---|---|
| **network** | Укажите для аккаунтинга сервисных запросов, касающихся сети. |
| **start-stop** | Указывает на отправку accounting-сообщений как при входе, так и при выходе из системы. Пользователям разрешен доступ к сети независимо от того, успешно ли активирован акккаунтинг при отправке начального accounting-сообщения. |
| **default** | Указывает на настройку списка методов аккаунтинга сетевых ресурсов по умолчанию. |
| *METHOD1* **[***METHOD2***...]** | Укажите список методов, который необходимо выполнить алгоритму аккаунтинга в заданной последовательности. Введите от одного до четырех методов. Для установки метода используйте ключевые слова.<br>**group radius** – используются серверы, определенные командой RADIUS server host.<br>**group tacacs+** – используются серверы, определенные командой TACACS+ server host.<br>**group** *GROUP-NAME* – используются группы серверов, определенные командой AAA group server.<br>**none** – аккаунтинг не выполняется. |

**По умолчанию**

Метод аккаунтинга AAA не настроен.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

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

**Пример**

В данном примере показано, как включить аккаунтинг платы за обеспечение доступа к сети, используя RADIUS, который будет отправлять accounting-сообщения, когда пользователь входит и отключается от системы.

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

## *7.4. aaa accounting system*

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

**aaa accounting system default start-stop** *METHOD1* **[***METHOD2***...]**

**no aaa accounting system default**

**Параметры**

| | |
|---|---|
| **system** | Указывает на выполнение аккаунтинга событий системного уровня. |
| **start-stop** | Указывает на отправку accounting-сообщений как при входе, так и при выходе из системы. Пользователям разрешен доступ к сети независимо от того, успешно ли активирован акккаунтинг при отправке начального accounting-сообщения. |
| **default** | Указывает на настройку списка методов аккаунтинга системных ресурсов по умолчанию. |
| *METHOD1* **[***METHOD2***...]** | Укажите список методов, который необходимо выполнить алгоритму аккаунтинга в заданной последовательности. Введите от одного до четырех методов. Для установки метода используйте ключевые слова.<br>**group radius** – используются серверы, определенные командой RADIUS server host.<br>**group tacacs+** – используются серверы, определенные командой TACACS+ server host.<br>**group** *GROUP-NAME* – используются группы серверов, определенные командой AAA group server.<br>**none** – аккаунтинг не выполняется. |

**По умолчанию**

Метод аккаунтинга AAA не настроен.

**Режим ввода команды**

Global Configuration Mode

**Уровень команды по умолчанию**

Уровень 15

**Использование команды**

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

**Пример**

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

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

## *7.5. aaa authentication enable*

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

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

**no aaa authentication enable default**

**Параметры**

| | |
|---|---|
| *METHOD1* **[***METHOD2***...]** | Укажите список методов, который необходимо выполнить алгоритму аутентификации в заданной последовательности. Введите от одного до четырех методов. Для установки метода используйте ключевые слова.<br><br>**enable** – для аутентификации используется локальный пароль.<br><br>**group radius** – используются серверы, определенные командой RADIUS server host.<br><br>**group tacacs+** – используются серверы, определенные командой TACACS+ server host.<br><br>**group** *GROUP-NAME* – используются группы серверов, определенные командой AAA group server.<br><br>**none** – как правило, данный метод указывается в списке последним. 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 установки списка методов аутентификации по умолчанию, чтобы настроить доступ к привилегированному уровню EXEC при вводе команды **enable [privilege** *LEVEL***]**. Аутентификация с использованием RADIUS-сервера основана на уровне привилегий и в качестве имени пользователя использует “enable12” или “enable15”.

**Пример**

В данном примере показано, как установить список методов аутентификации по умолчанию. Метод работает с группой серверов “group2”.

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

## *7.6. aaa authentication dot1x*

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

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

**no aaa authentication dot1x default**

**Параметры**

| | |
|---|---|
| *METHOD1* **[***METHOD2***...]** | Укажите список методов, который необходимо выполнить алгоритму аутентификации в заданной последовательности. Введите от одного до четырех методов. Для установки метода используйте ключевые слова.<br><br>**local** – для аутентификации используется локальная база данных.<br><br>**group radius** – используются серверы, определенные командой RADIUS server host.<br><br>**group** *GROUP-NAME* – используются группы серверов, определенные командой AAA group server.<br><br>**none** – как правило, данный метод указывается в списке последним. 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 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)#
```

## *7.7. aaa authentication login*

Данная команда используется для настройки списка методов аутентификации при входе в систему. Используйте форму **no** для удаления списка методов.

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

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

**Параметры**

| | |
|---|---|
| **default** | Указывается, чтобы использовать для аутентификации список методов по умолчанию. |
| *LIST-NAME* | Указывается имя списка методов, отличного от списка методов по умолчанию. Длина имени не должна превышать 32 символов. |
| *METHOD1* **[***METHOD2***...]** | Укажите список методов, который необходимо выполнить алгоритму аутентификации в заданной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для установки метода.<br><br>**local** – для аутентификации используется локальная база данных.<br><br>**group radius** – используются серверы, определенные командой |

| | |
|---|---|
| | RADIUS server host.<br><br>**group tacacs+** – используются серверы, определенные командой TACACS+ server host.<br><br>**group** *GROUP-NAME* – используются группы серверов, определенные командой AAA group server.<br><br>**none** – как правило, данный метод указывается в списке последним. 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, используемого для аутентификации при входе в систему. Можно настроить несколько списков методов. Для определения списка по умолчанию используется ключевое слово по умолчанию.

Если для аутентификации задан несуществующий список методов по умолчанию, то аутентификация выполняется на основе локальной базы данных.

При входе в систему с данным типом аутентификации проверяется имя пользователя и пароль, а также назначается уровень привилегий пользователя на основе базы данных.

Список методов является последовательным списком, описывающим методы аутентификации, которые должны запрашиваться для того, чтобы аутентифицировать пользователя. Списки методов позволяют назначить один или несколько протоколов безопасности, которые должны использоваться для аутентификации, что обеспечивает резервную систему аутентификации в случае сбоя исходного метода. Для аутентификации пользователей используется первый метод в списке. Если этот метод не отвечает, система переходит к следующему методу аутентификации в списке. Этот процесс продолжается до тех пор, пока не будет установлено успешное соединение с помощью метода аутентификации из списка, или пока все методы, перечисленные в списке, не будут исчерпаны.

Система переходит к следующему методу аутентификации по списку, только когда от предыдущего метода не поступает ответа. Если в любой момент данного цикла происходит сбой аутентификации, т.е. сервер безопасности или локальная база данных отвечает пользователю отказом в доступе, то процесс аутентификации останавливается, и другие методы аутентификации дальше не применяются.

**Пример**

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

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

## *7.8. aaa authentication mac-auth*

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

**aaa authentication mac-auth default** *METHOD1* **[***METHOD2***...]**

**no aaa authentication mac-auth default**

**Параметры**

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

**По умолчанию**

Метод аутентификации AAA не настроен.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

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

**Пример**

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

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

## *7.9. aaa authentication web-auth*

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

**aaa authentication web-auth default** *METHOD1* **[***METHOD2***...]**

**no aaa authentication web-auth default**

**Параметры**

| | |
|---|---|
| *METHOD1* **[***METHOD2***...]** | Укажите список методов, который необходимо выполнить алгоритму аутентификации в заданной последовательности. Введите от одного до четырех методов. Для установки метода используйте ключевые слова.<br><br>**local** – для аутентификации используется локальная база данных.<br><br>**group radius** – используются серверы, определенные командой RADIUS server host.<br><br>**group** *GROUP-NAME* – используются группы серверов, определенные командой AAA group server.<br><br>**none** – как правило, данный метод указывается в списке последним. Пользователь пройдет аутентификацию, если это не запрещено ему предыдущим методом аутентификации. |

**По умолчанию**

Метод аутентификации AAA не настроен.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

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

**Пример**

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

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

## *7.10. aaa group server radius*

Данная команда используется для входа в режим настройки группы серверов RADIUS и привязки серверов к группе. Используйте форму **no** для удаления группы серверов RADIUS.

**aaa group server radius** *GROUP-NAME*

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

**Параметры**

| | |
|---|---|
| *GROUP-NAME* | Имя группы серверов. Длина имени не должна превышать 32 символов. Синтаксисом является обычная строка без пробелов. |

**По умолчанию**

Группа серверов AAA не настроена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Используйте данную команду для назначения группы серверов RADIUS. Созданная группа серверов используется для установки списков методов, используемых для аутентификации или аккаунтинга с помощью команд **aaa authentication** и **aaa accounting**. Также используйте данную команду для входа в режим настройки группы серверов RADIUS (RADIUS Group Server Configuration Mode). Используйте команду **server** для привязки серверов RADIUS к группе.

**Пример**

В данном примере показано, как создать группу серверов RADIUS с двумя записями. Вторая запись 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)#
```

## *7.11. aaa group server tacacs+*

Данная команда используется для входа в режим настройки группы серверов TACACS+ и привязки серверов к группе. Используйте форму **no** для удаления группы серверов TACACS+.

**aaa group server tacacs+** *GROUP-NAME*

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

**Параметры**

| | |
|---|---|
| *GROUP-NAME* | Имя группы серверов. Длина имени не должна превышать 32 символов. Синтаксисом является обычная строка без пробелов. |

**По умолчанию**

Группа серверов AAA не настроена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Используйте данную команду для входа в режим настройки группы серверов TACACS+. Используйте команду **server** для привязки серверов TACACS+ к группе. Заданная группа серверов может быть указана в качестве списка методов для аутентификации или аккаунтинга с помощью команд **aaa authentication** и **aaa accounting**.

**Пример**

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

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

## *7.12. aaa new-model*

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

**aaa new-model**

**no aaa new-model**

**Параметры**

Нет.

**По умолчанию**

По умолчанию данная функция отключена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Используйте команду **aaa new-model** для включения функции AAA. Функция должна быть включена до того, как начнет действовать аутентификация и аккаунтинг по спискам методов AAA. Если функция AAA отключена, пользователь будет аутентифицирован через локальную таблицу учетных записей, созданную командой **username**. Пароль для входа в систему будет аутентифицирован через локальную таблицу, которая определяется командой **enable password**.

**Пример**

В данном примере показано, как включить функцию AAA.

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

## *7.13. accounting commands*

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

**accounting commands** *LEVEL* **{default |** *METHOD-LIST***}**

**no accounting commands** *LEVEL*

**Параметры**

| | |
|---|---|
| *LEVEL* | Укажите уровень привилегий, на котором необходим аккаунтинг всех команд **configure**. Допустимые уровни привилегий: от 1 до 15. |
| **default** | Указывается для ведения аккаунтинга на основе списка методов по умолчанию. |
| *METHOD-LIST* | Имя определенного списка методов. |

**По умолчанию**

По умолчанию данная опция отключена.

**Режим ввода команды**

Line Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Чтобы аккаунтинг по списку методов вступил в силу, предварительно включите функцию AAA, используя команду **aaa new-model**. Заранее создайте список методов, используя команду **aaa accounting commands**. Если список методов отсутствует, то команда не вступает в силу. Доступно использование разных списков методов для аккаунтинга команд на разных уровнях. Для одного уровня может быть указан только один список методов.

**Пример**

В данном примере показано, как включить аккаунтинг команд, вводимых через консоль, на 15 уровне привилегий, с использованием списка методов “cmd-15”.

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

## *7.14. accounting exec*

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

**accounting exec {default |** *METHOD-LIST***}**

**no accounting exec**

**Параметры**

| | |
|---|---|
| **default** | Указывается для использования списка методов по умолчанию. |
| *METHOD-LIST* | Имя определенного списка методов. |

**По умолчанию**

По умолчанию данная опция отключена.

**Режим ввода команды**

Line Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

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

**Пример**

В данном примере показано, как настроить список методов аккаунтинга EXEC с именем “list-1”, использующий сервер RADIUS. Если сервер безопасности не отвечает, аккаунтинг не выполняется. После настройки аккаунтинг EXEC применяется к консоли.

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

## *7.15. clear aaa counters servers*

Данная команда используется для сброса счетчиков статистики серверов AAA.

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

**Параметры**

| | |
|---|---|
| **all** | Обнуляет счетчики для всех серверов. |
| **radius** *IP-ADDRESS* | Обнуляет счетчики для заданного сервера RADIUS IPv4. |
| **radius** *IPV6-ADDRESS* | Обнуляет счетчики для заднного сервера RADIUS IPv6. |
| **radius all** | Обнуляет счетчики для всех серверов RADIUS. |
| **tacacs** *IP-ADDRESS* | Обнуляет счетчики для заданного сервера TACACS IPv4. |
| **tacacs** *IPV6-ADDRESS* | Обнуляет счетчики для заданного сервера TACACS IPv6. |
| **tacacs all** | Обнуляет счетчики для всех серверов TACACS. |
| **sg** *NAME* | Обнуляет счетчики для всех серверов в указанной группе. |

**По умолчанию**

Нет.

**Режим ввода команды**

Privileged EXEC Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

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

**Пример**

В данном примере показано, как сбросить счетчики серверов AAA.

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

В данном примере показано, как удалить информацию счетчиков серверов AAA для всех узлов в группе серверов “server-farm”.

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

## *7.16. ip http authentication aaa login-authentication*

Данная команда используется для назначения списка методов аутентификации AAA для аутентификации пользователей HTTP-сервера. Используйте форму **no** для возврата к списку методов по умолчанию.

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

**no ip http authentication aaa login-authentication**

**Параметры**

| | |
|---|---|
| **default** | Указывается для аутентификации на основе списка методов по умолчанию. |
| *METHOD-LIST* | Указывается имя определнного списка методов. |

**По умолчанию**

По умолчанию используется опция **default**.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Чтобы аутентификация по списку методов вступила в силу, предварительно включите функцию AAA, используя команду **aaa new-model**. Заранее создайте список методов, используя команду **aaa authentication login**. Если список методов отсутствует, то команда не вступает в силу, и аутентификация будет выполняться по списку методов по умолчанию, созданному командой **aaa authentication login default**.

**Пример**

В данном примере показано, как настроить сессии HTTP для использования списка методов “WEB-METHOD” для аутентификации при входе.

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

## *7.17. ip http accounting exec*

Данная команда используется для назначения метода аккаунтинга AAA для пользователей HTTP-сервера. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**ip http accounting exec {default |** *METHOD-LIST***}**

**no ip http accounting exec**

**Параметры**

| | |
|---|---|
| **default** | Указывается для ведения аккаунтинга на основе списка методов по умолчанию. |
| *METHOD-LIST* | Указывается имя определенного списка методов. |

**По умолчанию**

По умолчанию данная опция отключена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

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

**Пример**

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

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

## *7.18. ip radius source-interface*

Данная команда используется для назначения интерфейса, чей IP-адрес будет использоваться в качестве IP-адреса источника для отправки пакетов RADIUS. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**ip radius source-interface** *INTERFACE-ID*

**no ip radius source-interface**

**Параметры**

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

**По умолчанию**

Используется IP-адрес ближайшего интерфейса.

**Режим ввода команды**

Global Configuration Mode.

Server Group Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Данная команда применяется для назначения интерфейса, чей IP-адрес будет использоваться в качестве IP-адреса источника для отправки пакетов RADIUS. Если интерфейс источника указан как в режиме глобальной конфигурации (Global Configuration mode), так и в режиме конфигурации группы серверов (Group Server Configuration mode), то интерфейс источника, указанный в режиме конфигурации группы серверов, обладает приоритетом.

Когда сервер находится на порту управления Out-Of-Band, в качестве интерфейса источника для отправки запросов на порт управления необходимо указать идентификатор интерфейса (Interface ID) порта управления Out-Of-Band.

**Пример**

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

```
Switch#configure terminal
Switch(config)# ip radius source-interface vlan100
Switch(config)#
```

## *7.19. ip tacacs source-interface*

Данная команда используется для назначения интерфейса, чей IP-адрес будет использоваться в качестве IP-адреса источника для отправки пакетов TACACS. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**ip tacacs source-interface** *INTERFACE-ID*

**no ip tacacs source-interface**

**Параметры**

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

**По умолчанию**

Используется IP-адрес ближайшего интерфейса.

**Режим ввода команды**

Global Configuration Mode.

Server Group Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Данная команда может применяться для назначения интерфейса, чей IP-адрес будет использоваться в качестве IP-адреса источника для отправки пакетов TACACS. Если интерфейс источника указан как в режиме глобальной конфигурации, так и в режиме конфигурации группы серверов, то интерфейс источника, указанный в режиме конфигурации группы серверов, обладает приоритетом.

Когда сервер находится на порту управления Out-Of-Band, в качестве интерфейса источника для отправки пакета с запросом на порт управления необходимо указать идентификатор интерфейса порта управления Out-Of-Band.

**Пример**

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

```
Switch#configure terminal
Switch(config)# ip tacacs source-interface vlan100
Switch(config)#
```

## *7.20. ip vrf forwarding (server-group)*

Данная команда используется в режиме конфигурации группы серверов для назначения VRF группам серверов AAA RADIUS или TACACS+. Используйте форму **no**, чтобы группы серверов могли использовать таблицы маршрутизации по умолчанию.

**ip vrf forwarding** *VRF-NAME*

**no ip vrf forwarding**

**Параметры**

| | |
|---|---|
| *VRF-NAME* | Имя VRF (Virtual Routing and Forwarding). |

**По умолчанию**

По умолчанию используется глобальная таблица маршрутизации.

**Режим ввода команды**

Server Group Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Используйте данную команду для назначения VRF группе серверов AAA RADIUS или TACACS+. Данная команда позволяет пользователям доступа использовать серверы AAA в разных доменах маршрутизации.

**Пример**

В данном примере показано, как указать VRF для группы серверов RADIUS.

```
Switch#configure terminal
Switch(config)#aaa group server radius_global
Switch(config-sg-radius)#server 172.16.10.254
Switch(config-sg-radius)#exit
Switch(config)#
Switch(config)#aaa group server radius_sales
Switch(config-sg-radius)#server 10.10.0.1
Switch(config-sg-radius)#ip vrf forwarding sales
Switch(config-sg-radius)#
```

## *7.21. ipv6 radius source-interface*

Данная команда используется для назначения интерфейса, чей IPv6-адрес будет использоваться в качестве IPv6-адреса источника для отправки пакетов RADIUS. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**ipv6 radius source-interface** *INTERFACE-ID*

**no ipv6 radius source-interface**

**Параметры**

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

**По умолчанию**

Используется IPv6-адрес ближайшего интерфейса.

**Режим ввода команды**

Global Configuration Mode.

Server Group Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Данная команда применяется для назначения интерфейса, чей IPv6-адрес будет использоваться в качестве IPv6-адреса источника для отправки пакетов RADIUS. Если интерфейс источника указан как в режиме глобальной конфигурации, так и в режиме конфигурации группы серверов, то интерфейс источника, указанный в режиме конфигурации группы серверов, обладает приоритетом.

Когда сервер находится на порту управления Out-Of-Band, в качестве интерфейса источника для отправки пакета с запросом на порт управления необходимо указать идентификатор интерфейса (Interface ID) порта управления Out-Of-Band.

**Пример**

В данном примере показано, как установить VLAN100, чей IPv6-адрес будет использоваться в качестве IP-адреса источника для отправки пакетов RADIUS.

```
Switch#configure terminal
Switch(config)# ipv6 radius source-interface vlan100
Switch(config)#
```

## *7.22. login authentication*

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

**login authentication {default |** *METHOD-LIST***}**

**no login authentication**

**Параметры**

| | |
|---|---|
| **default** | Указывается для аутентификации на основе списка методов по умолчанию. |
| *METHOD-LIST* | Указывается имя определенного списка методов. |

**По умолчанию**

По умолчанию используется список методов по умолчанию.

**Режим ввода команды**

Line Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Чтобы аутентификация по списку методов вступила в силу, предварительно включите функцию AAA, используя команду **aaa new-model**. Заранее создайте список методов, используя команду **aaa authentication login**. Если список методов отсутствует, то команда не вступает в силу, и аутентификация будет выполняться по списку методов по умолчанию, созданному командой **aaa authentication login default**.

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

**Пример**

В данном примере показано, как установить локальную сессию консоли для использования списка методов “CONSOLE-LINE-METHOD” для аутентификации при входе.

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

## *7.23. radius-server attribute 4*

Данная команда применяется для назначения IP-адреса, используемого в качестве значения параметра RADIUS attribute 4. Используйте форму **no** для удаления IP-адреса.

**radius-server attribute 4** *IP-ADDRESS*

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

**Параметры**

| | |
|---|---|
| *IP-ADDRESS* | IP-адрес для RADIUS attribute 4. |

**По умолчанию**

По умолчанию IP-адресом является IP-адрес на интерфейсе, который подключает NAS к серверу RADIUS.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Обычно, когда настроена команда **ip radius source-interface**, указанный IP-адрес используется в IP-заголовках пакетов RADIUS, а также в качестве значения RADIUS attribute 4 address.

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

Если настроены обе команды, указанный в команде **radius-server attribute 4** IP-адрес используется в качестве адреса RADIUS attribute 4 внутри пакета RADIUS. IP-адрес на интерфейсе, заданный в команде **ip radius-source interface,** используется в качестве IP-адреса в IP-заголовках пакетов RADIUS.

**Пример**

В данном примере показано, как настроить IP-адрес 10.0.0.21 в качестве атрибута RADIUS NAS-IP-Address.

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

## *7.24. radius-server deadtime*

Данная команда используется для назначения интервала времени, в течение которого разрешается пропускать опрос недоступного сервера. Используйте форму **no,** чтобы вернуть настройки по умолчанию.

**radius-server deadtime** *MINUTES*

**no radius-server deadtime**

**Параметры**

| | |
|---|---|
| *MINUTES* | Время простоя. Допустимый диапазон: от 0 до 1440 (24 часа). Если установлено значение 0, недоступный сервер 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 позволяет оптимизировать время обработки данных аутентификации с помощью установки времени простоя (deadtime), в течение которого недоступные серверы опрашиваться не будут.

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

**Пример**

В примере ниже показано, как установить время простоя на 10 минут.

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

## *7.25. radius-server host*

Данная команда используется для добавления RADIUS-сервера в список используемых серверов. Используйте форму **no** для удаления сервера.

**radius-server host {***IP-ADDRESS* **|** *IPV6-ADDRESS***} [auth-port** *PORT***] [acct-port** *PORT***] [timeout** *SECONDS***] [retransmit** *COUNT***] key [0 | 7]** *KEY-STRING*

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

**Параметры**

| | |
|---|---|
| *IP-ADDRESS* | IP-адрес RADIUS-сервера. |
| IPV6-ADDRESS | IPv6-адрес RADIUS-сервера. |
| **auth-port** *PORT-NUMBER* | (Опционально) Номер UDP-порта назначения для отправки пакетов аутентификации. Диапазон: от 0 до 65535. Установите номер порта в ноль, если сервер не предназначен для аутентификации. Значение по умолчанию: 1812. |
| **acct-port** *PORT-NUMBER* | (Опционально) Номер UDP-порта назначения для отправки пакетов аккаунтинга. Диапазон: от 0 до 65535. Установите номер порта в ноль, если сервер не предназначен для аккаунтинга. Значение по умолчанию: 1813. |

| | |
|---|---|
| **timeout** *SECONDS* | Значение тайм-аута сервера. Диапазон: от 1 до 255 секунд. Если значение не указано, то значением по умолчанию является 5 секунд. |
| **retransmit** *COUNT* | (Опционально) Количество повторных передач запросов на сервер, когда ответ не получен. Значение: от 0 до 20. Используйте 0 для отключения повторной передачи. Если значение не указано, то значением по умолчанию является 2. |
| **0** | (Опционально) Пароль в форме обычного незашифрованного текста. Это является опцией по умолчанию. |
| **7** | (Опционально) Пароль в зашифрованной форме. |
| **key** *KEY-STRING* | Ключ, используемый для связи с сервером. Длина ключа может составлять от 1 до 32 символов незашифрованного текста. |

**По умолчанию**

По умолчанию сервер не настроен.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

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

**Пример**

В данном примере показано, как задать два RADIUS-сервера 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)#
```

## *7.26. server (RADIUS)*

Данная команда используется для привязки RADIUS-сервера к группе RADIUS-серверов. Используйте форму **no** для удаления сервера из группы.

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

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

**Параметры**

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

**По умолчанию**

По умолчанию сервер не настроен.

**Режим ввода команды**

RADIUS Group Server Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Используйте данную команду для входа в режим настройки группы серверов RADIUS (RADIUS Group Server Configuration Mode). Используйте команду **server** для привязки RADIUS-сервера к группе серверов RADIUS. Определенная группа серверов может быть указана в качестве списка методов аутентификации или аккаунтинга с помощью команд **aaa authentication** и **aaa accounting**. Используйте команду **radius-server host** для создания записи сервера. Данная запись идентифицируется по IP-адресу.

**Пример**

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

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

## *7.27. server (TACACS+)*

Данная команда используется для привязки сервера TACACS+ к группе серверов. Используйте форму **no** для удаления сервера из группы.

**server** *IP-ADDRESS*

**no server** *IP-ADDRESS*

**Параметры**

| | |
|---|---|
| *IP-ADDRESS* | IPv4-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 привязки сервера TACACS+ к группе серверов TACACS+. Определенная группа серверов может быть указана в качестве списка методов для аутентификации или аккаунтинга с помощью команд **aaa authentication** и **aaa accounting**. Используйте команду **tacacs-server host** для создания записи сервера. Данная запись идентифицируется по IP-адресу.

**Пример**

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

```
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+)#
```

## *7.28. show aaa*

Данная команда используется для отображения глобального состояния AAA.

**show aaa**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

Privileged EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Используйте эту команду для отображения глобального состояния AAA.

**Пример**

В данном примере показано, как отобразить глобальное состояние AAA.

```
Switch# show aaa

AAA is enabled.

Switch#
```

## *7.29. tacacs-server host*

Данная команда используется для добавления сервера TACACS+ в список используемых серверов. Используйте форму **no** для удаления сервера.

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

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

**Параметры**

| | |
|---|---|
| *IP-ADDRESS* | IPv4-адрес сервера TACACS+. |
| IPV6-ADDRESS | IPv6-адрес сервера TACACS+. |

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

**По умолчанию**

По умолчанию узел сервера TACACS+ не настроен.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

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

**Пример**

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

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

## *7.30. show radius statistics*

Данная команда отображает статистику RADIUS для пакетов аккаунтинга и аутентификации.

**show radius statistics**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

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

**Отображаемые параметры**

| | |
|---|---|
| **Auth.** | Статистика для пакетов аутентификации. |
| **Acct.** | Статистика для пакетов аккаунтинга. |
| **Round Trip Time** | Интервал времени (в сотых долях секунды) между 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 отправленных данному RADIUS-серверу. Повторные передачи включают попытки, при которых поля Identifier и Acct-Delay были обновлены, а также попытки, при которых они остаются без изменений. |
| **Malformed Responses** | Количество ошибочных пакетов RADIUS Response, полученных от данного сервера. Ошибочные пакеты включают пакеты с некорректной длиной. Некорректные аутентификаторы или атрибуты Signature, а также неизвестные типы не учитываются. |
| **Bad Authenticators** | Количество пакетов RADIUS Response, полученных от данного сервера и содержащих некорректные аутентификаторы или атрибуты Signature. |
| **Pending Requests** | Количество пакетов RADIUS Request, предназначенных для данного сервера, время ожидания которых еще не истекло, или которые не получили ответ. Эта переменная увеличивается, когда запрос отправляется, и уменьшается из-за получения ответа, тайм-аута или повторной передачи. |
| **Timeouts** | Количество тайм-аутов для данного сервера. По истечении тайм-аута клиент может повторить попытку подключения к данному серверу, отправить запрос на аутентификацию другому серверу или прекратить попытки. Повторная попытка подключиться к этому же серверу считается повторной передачей, так же как и тайм-аут. Попытка подключиться к другому серверу рассматривается как запрос, точно так же как и тайм-аут. |
| **Unknown Types** | Количество пакетов RADIUS неизвестного типа, полученных от данного сервера. |
| **Packets Dropped** | Количество пакетов RADIUS, полученных от данного сервера и отброшенных по какой-либо причине. |

## *7.31. show tacacs statistics*

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

**show tacacs statistics**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

Privileged EXEC Mode.

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

**Отображаемые параметры**

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

# 8. Базовые команды настройки IPv4

## *8.1. arp*

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

**arp [vrf** *VRF-NAME***]** *IP-ADDRESS HARDWARE-ADDRESS*

**no arp [vrf** *VRF-NAME***]** *IP-ADDRESS HARDWARE-ADDRESS*

**Параметры**

| | |
|---|---|
| **vrf** *VRF-NAME* | (Опционально) Укажите имя VRF instance. |
| *IP-ADDRESS* | Укажите IP-адрес. |
| *HARDWARE-ADDRESS* | Укажите MAC-адрес (48-битный). |

**По умолчанию**

В кэше ARP нет ни одной статической записи.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

В примере показан процесс добавления статической ARP-записи для традиционного Ethernet-узла.

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

## *8.2. arp timeout*

Данная команда используется для настройки времени старения (aging time) ARP-записей в таблице ARP. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**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. Если указать 0, то записи ARP никогда не устаревают. |

**По умолчанию**

По умолчанию установлено 240 минут.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

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

```
Switch# configure terminal
Switch(config)# interface 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 [vrf** *VRF-NAME*] **{all | interface** *INTERFACE-ID* **|** *IP-ADDRESS*}

**Параметры**

| | |
|---|---|
| **vrf** *VRF-NAME* | (Опционально) Укажите имя VRF instance. |
| **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 основного или второстепенного адреса IPv4, а также для автоматического получения IP-адреса от DHCP-сервера. Используйте форму **no**, чтобы удалить настройки IP-адреса или отключить DHCP на интерфейсе.

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

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

**Параметры**

| | |
|---|---|
| *IP-ADDRESS* | Укажите IP-адрес. |
| *SUBNET-MASK* | Укажите маску подсети для соответствующего IP-адреса. |
| **secondary** | (Опционально) Укажите, если настроенный адрес является второстепенным IP-адресом. Если данное ключевое слово не указано, настроенный адрес будет являться основным IP-адресом. |
| **dhcp** | Укажите, чтобы получить IP-адрес от DHCP-сервера. |

**По умолчанию**

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

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

IPv4-адрес интерфейса может быть 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, 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, а 192.31.7.17 и 192.31.8.17 в качестве второстепенных адресов для VLAN 100.

```
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 secondary
Switch(config-if)# ip address 192.31.8.17 255.255.255.0 secondary
Switch(config-if)#
```

## *8.5. ip proxy-arp*

Данная команда используется для включения опции proxy ARP для интерфейса. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**ip proxy-arp**

**no ip proxy-arp**

**Параметры**

Нет.

**По умолчанию**

Данная опция по умолчанию отключена.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте данную команду для настройки на интерфейсе опции proxy ARP. При включении этой опции система будет отвечать на запросы ARP для IP-адресов локальных подсетей. Механизм proxy ARP может использоваться в сети, где для узлов не настроен шлюз по умолчанию.

**Пример**

В данном примере показано, как включить proxy ARP для интерфейса VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan100
Switch(config-if)# ip proxy-arp
Switch(config-if)#
```

## *8.6. ip local-proxy-arp*

Данная команда используется для включения на интерфейсе опции local proxy ARP. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**ip local-proxy-arp**

**no ip local-proxy-arp**

**Параметры**

Нет.

**По умолчанию**

Данная опция по умолчанию отключена.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12, 15.

**Использование команды**

Используйте данную команду для включения опции local proxy ARP на интерфейсе. Команда используется в основной VLAN, относящейся к домену изолированной сети VLAN, для включения маршрутизации пакетов между второстепенными сетями VLAN или изолированными портами в пределах домена. Команда сработает только после включения опции **ip arp proxy**.

**Пример**

В примере ниже показано, как включить local proxy ARP на интерфейсе VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan100
Switch(config-if)# ip local-proxy-arp
Switch(config-if)#
```

## *8.7. ip arp elevation*

Данная команда используется для назначения более высокого приоритета всем ARP-пакетам этого коммутатора по сравнению с остальными ARP-пакетами.

**ip arp elevation**

**no ip arp elevation**

**Параметры**

Нет.

**По умолчанию**

По умолчанию все ARP-пакеты имеют одинаковый приоритет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте данную команду для назначения всем ARP-пакетам этого коммутатора более высокого приоритета по сравнению с остальными ARP-пакетами.

**Пример**

В данном примере показано, как включить повышение приоритета IP ARP.

```
Switch# configure terminal
Switch(config)# ip arp elevation
Switch(config)#
```

## *8.8. ip mtu*

Данная команда используется для настройки значения MTU. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**ip mtu** *BYTES*

**no ip mtu**

**Параметры**

| | |
|---|---|
| *BYTES* | Укажите значение IP MTU. Диапазон допустимых значений: от 512 до 16383 байт. |

**По умолчанию**

По умолчанию установлено значение MTU = 1500 байт.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Некоторые протоколы маршрутизации, такие как OSPF, будут анонсировать этот параметр в обновлениях маршрутов.

**Пример**

В данном примере показано, как задать значение MTU размером 6000 байт для VLAN 4.

```
Switch# configure terminal
Switch(config)# interface vlan4
Switch(config-if) ip mtu 6000
Switch(config-if)#
```

## *8.9. show arp*

Данная команда используется для отображения данных кэша ARP.

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

**Параметры**

| | |
|---|---|
| **vrf** *VRF-NAME* | (Опционально) Укажите имя VRF instance. |
| *ARP-TYPE* | (Опционально) Укажите тип ARP.<br>**dynamic** – для отображения только динамических ARP-записей.<br>**static** – для отображения только статических ARP-записей. |
| *IP-ADDRESS [MASK]* | (Опционально) Укажите, если необходимо отобразить определенную запись или записи определенной сети. |
| *INTERFACE-ID* | (Опционально) Укажите, если необходимо отобразить ARP-записи, связанные с определенной сетью. |
| *HARDWARE-ADDRESS* | (Опционально) Укажите, если необходимо отобразить ARP-записи, чей аппаратный адрес равен данному MAC-адресу. |

**По умолчанию**

Нет.

**Режим ввода команды**

User 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 примере ниже показано, как отобразить данные кэша ARP.

```
Switch# show arp

S - Static Entry
IP Address                Hardware Addr       IP Interface     Age (min)
--------------------------------------------------------------------------
S 10.108.42.112           00-00-a7-10-4b-af   vlan100          forever
10.108.42.114             00-00-a7-10-85-9b   vlan200          forever
10.108.42.121             00-00-a7-10-68-cd   vlan300          125

Total Entries: 3

Switch#
```

## *8.10. show arp timeout*

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

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

**Параметры**

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

**По умолчанию**

Нет.

**Режим ввода команды**

User 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)
---------------------------------------
vlan100                30
vlan200                40

Total Entries: 2

Switch#
```

## *8.11. 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-интерфейсам. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Если идентификатор интерфейса не указан, будет отображаться информация для всех интерфейсов.

**Пример**

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

```
Switch# show ip interface brief

Interface           IP-Address      Link Status
------------------- --------------- ----------
vlan1               10.90.90.90     up
vlan2               20.1.1.1        up

Total Entries: 2

Switch#
```

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

```
Switch# show ip interface vlan 1

Interface vlan1 is enabled, Link status is up
  IP address is 10.90.90.90/8 (Manual)
  ARP timeout is 240 minutes.
  IP MTU is 1500 bytes
  Helper Address is not set
  Proxy ARP is disabled
  IP Local Proxy ARP is disabled
  IP Directed Broadcast is disabled
  gratuitous-send is disabled, interval is 0 seconds

Total Entries: 1

Switch#
```

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

```
Switch# show ip interface loopback 1

Interface loopback1 is enabled,
  IP address is 10.0.0.1/24 (Manual)

Total Entries: 1

Switch#
```

## *8.12. ip directed-broadcast*

Данная команда используется для включения преобразования направленных широковещательных рассылок, получаемых интерфейсом, в рассылки канального уровня, когда сеть назначения подключена непосредственно к коммутатору. Используйте форму **no**, чтобы отключить преобразование.

**ip directed-broadcast**

**no ip directed-broadcast**

**Параметры**

Нет.

**По умолчанию**

Данная опция по умолчанию отключена.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте данную команду для настройки на интерфейсе направленной широковещательной рассылки. Данная команда не влияет на маршрутизацию одноадресных пакетов, передачу пакетов направленной широковещательной рассылки за пределы локальной сети.

Данная команда влияет только на передачу пакетов направленной широковещательной рассылки, для которых сетями назначения являются локальные подсети коммутатора. При включении опции направленной широковещательной рассылки пакеты буду преобразованы в широковещательные и направлены всем узлам сети назначения. В качестве интерфейса отправки может использоваться интерфейс получения или другие интерфейсы коммутатора.

**Пример**

В данном примере показано, как включить направленную широковещательную рассылку для интерфейса VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan100
Switch(config-if)# ip directed-broadcast
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 для удаления только динамических записей из IPv6 neighbor cache.

**Пример**

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

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

## *9.2. ipv6 address*

Данная команда используется для ручной настройки IPv6-адреса на интерфейсе. Используйте форму **no**, чтобы удалить заданный вручную IPv6-адрес.

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

**no ipv6 address {***IPV6-ADDRESS/PREFIX-LENGTH* | *PREFIX-NAME SUB-BITS/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. |
| *PREFIX-NAME* | Укажите имя префикса, используя не более 12 символов без пробелов. |
| *SUB-BITS* | Укажите сетевую и узловую части IPv6-адреса. |
| **link-local** | Укажите адрес Link-local. |

**По умолчанию**

Нет.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

Интерфейсу можно назначить несколько IPv6-адресов, используя для этого различные механизмы, включая ручную настройку, настройку адресов без сохранения состояния (Stateless address configuration) и настройку адресов с сохранением состояния (Stateful address configuration).

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

**Пример**

В данном примере показано, как задать IPv6-адрес.

```
Switch# configure terminal
Switch(config)# interface vlan2
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 vlan2
Switch(config-if)# no ipv6 address 3ffe:22:3:44::55/64
```

В данном примере показано, как настроить IPv6-адрес на базе основного префикса, полученного клиентом DHCPv6. Глобальный адрес будет сконфигурирован после получения клиентом DHCPv6 основного префикса. Предположим, что общий префикс – 2001:2:3/48, а итоговый IPv6-адрес – 2001:2:3:4:5::3/64.

```
Switch# configure terminal
Switch(config)# interface vlan2
Switch(config-if)# ipv6 address dhcp-prefix  1:2:3:4:5::3/64
```

В данном примере показано, как отменить формирование IPv6-адреса на основе префикса, полученного DHCPv6-клиентом.

```
Switch# configure terminal
Switch(config)# interface vlan2
Switch(config-if)# no ipv6 address dhcp-prefix 0:0:0:2::3/64
```

## *9.3. ipv6 address autoconfig*

Данная команда используется для автоматической настройки IPv6-адреса с помощью механизма автоконфигурации Stateless Autoconfiguration. Используйте форму **no**, чтобы удалить IPv6-адрес, сгенерированный с помощью механизма автоконфигурации.

**ipv6 address autoconfig [default]**

**no ipv6 address autoconfig**

**Параметры**

| | |
|---|---|
| **default** | (Опционально.) Если на данном интерфейсе выбран параметр default router, то с помощью ключевого слова default можно установить маршрут по умолчанию, используя заданный default router. Ключевое слово **default** можно указать только на одном интерфейсе. |

**По умолчанию**

Данная опция по умолчанию отключена.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда доступна только для IPv6-адреса интерфейса VLAN. Опция автоконфигурации по умолчанию отключена.

При включении автоконфигурации интерфейс включает обработку IPv6 и получает анонс от маршрутизатора IPv6 с назначенным префиксом глобального адреса. Далее итоговый адрес, состоящий из префикса и идентификатора интерфейса, назначается данному интерфейсу. В случае отключения этой опции полученный Global Unicast-адрес будет удален из интерфейса.

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

**Пример**

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

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 address autoconfig
Switch(config-if)#
```

## *9.4. ipv6 address eui-64*

Данная команда используется для настройки на интерфейсе IPv6-адреса с использованием идентификатора интерфейса EUI-64 (Interface ID). Используйте форму **no**, чтобы удалить IPv6-адрес, сгенерированный с использованием идентификатора интерфейса EUI-64.

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

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

**Параметры**

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

**По умолчанию**

Нет.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

В данном примере показано, как добавить IPv6-адрес.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 address 3ffe:501:ffff:0::/64 eui-64
Switch(config-if)#
```

## *9.5. ipv6 address dhcp*

Данная команда используется для настройки интерфейса на получение IPv6-адреса с помощью DHCPv6. Используйте форму **no**, чтобы отключить использование DHCPv6 для получения IPv6-адреса.

**ipv6 address dhcp [rapid-commit]**

**no ipv6 address dhcp**

**Параметры**

| | |
|---|---|
| **rapid-commit** | Укажите, чтобы получать сетевые настройки от DHCP-сервера посредством быстрого обмена двумя сообщениями вместо стандартных четырех между Requesting Router (RR) и Delegating Router (DR). |

**По умолчанию**

Нет.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте данную команду для настройки интерфейса на получение сетевых настроек IPv6 от сервера DHCPv6. При использовании данной команды с формой **no** текущие сетевые настройки IPv6, полученные от DHCPv6-сервера, будут удалены. Если в команде указывается параметр **rapid-commit**, то в сообщение *SOLICIT* добавляется запрос на получение адреса посредством быстрого обмена двумя сообщениями вместо четырех.

**Пример**

В примере ниже показано, как настроить интерфейс VLAN1 на получение IPv6-адреса от

DHCPv6-сервера.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 address dhcp
Switch(config-if)#
```

## *9.6. ipv6 enable*

Данная команда используется для включения обработки Pv6 на интерфейсах, у которых нет явно настроенного IPv6-адреса. Используйте форму **no**, чтобы отключить обработку IPv6 на интерфейсах, у которых нет явно настроенного IPv6-адреса.

**ipv6 enable**

**no ipv6 enable**

**Параметры**

Нет.

**По умолчанию**

Данная опция по умолчанию отключена.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

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

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 enable
Switch(config-if)#
```

## *9.7. ipv6 hop-limit*

Данная команда используется для настройки параметра Hop Limit (Предельное число шагов) для IPv6. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**ipv6 hop-limit** *VALUE*

**no ipv6 hop-limit**

**Параметры**

| | |
|---|---|
| *VALUE* | Укажите диапазон значений для параметра IPv6 Hop Limit. Если задан 0, для отправки пакета используются настройки по умолчанию. Допустимые значения – от 0 до 255. |

**По умолчанию**

Значение по умолчанию – 64.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте данную команду для настройки параметра Hop Limit, который будет анонсироваться в сообщениях RA. Пакет IPv6, сгенерированный в системе, также будет использовать это значение в качестве начального значения параметра Hop Limit.

**Пример**

В данном примере показано, как задать значение Hop Limit для IPv6.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 hop-limit 255
Switch(config-if)#
```

## *9.8. ipv6 mtu*

Данная команда используется для настройки значения MTU для IPv6. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**ipv6 mtu** *BYTES*

**no ipv6 mtu**

**Параметры**

| | |
|---|---|
| *BYTES* | Укажите, чтобы задать значение MTU для IPv6. Допустимые значения – от 1280 до 65534 байт. |

**По умолчанию**

По умолчанию для IPv6 установлено значение MTU = 1500 байт.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда доступна только для конфигурации интерфейса L3. Используйте эту команду для настройки значения MTU, которое будет анонсироваться в сообщениях RA. Пакет IPv6, сгенерированный в системе, будет передаваться на основе этого значения. Проверка выполняется на выходе. Пакеты свыше 1518 байт (oversize) будут отправлены вышестоящему blade-серверу для дальнейшей обработки.

**Пример**

В данном примере показано, как задать значение IPv6 MTU размером 6000 байт для VLAN 4.

```
Switch# configure terminal
Switch(config)# interface vlan4
Switch(config-if) ipv6 mtu 6000
Switch(config-if)# exit
Switch(config)#
```

В примере ниже показано, как восстановить значение MTU, заданное по умолчанию.

```
Switch# configure terminal
Switch(config)# interface vlan4
Switch(config-if)# no ipv6 mtu
Switch(config-if)#
```

## *9.9. ipv6 nd managed-config-flag*

Данная команда используется для включения флага Managed Address Configuration (M) в анонсируемых сообщениях RA. Для выключения флага используйте форму **no**.

**ipv6 nd managed-config-flag**

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

**Параметры**

Нет.

**По умолчанию**

Данный функционал по умолчанию отключен.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

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

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 nd managed-config-flag
Switch(config-if)#
```

## *9.10. ipv6 nd other-config-flag*

Данная команда используется для включения флага Other Configuration (O) в анонсируемых сообщениях RA. Для выключения флага используйте форму **no**.

**ipv6 nd other-config-flag**

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

**Параметры**

Нет.

**По умолчанию**

Данный функционал по умолчанию отключен.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

В данном примере показано, как включить флаг O для получения других параметров конфигурации.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 nd other-config-flag
Switch(config-if)#
```

## *9.11. ipv6 nd prefix*

Данная команда используется для настройки IPv6-префикса, который будет анонсироваться в сообщениях RA. Для удаления префикса используйте форму **no**.

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

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

**Параметры**

| | |
|---|---|
| *IPV6-PREFIX/PREFIX-LENGTH* | Укажите IPv6-префикс, который будет сгенерирован или анонсирован в сообщении RA на интерфейсе. |
| *VALID-LIFETIME* | (Опционально.) Укажите период времени в секундах, в течение которого префикс будет действителен. Допустимые значения – от 0 до 4294967295. Если значение не задано, устанавливается значение по умолчанию – 2592000 секунд (30 дней). |
| *PREFERRED-LIFETIME* | (Опционально.) Укажите предпочтительное время жизни префикса в секундах. Допустимые значения – от 0 до 4294967295. Если значение не задано, устанавливается значение по умолчанию – 604 800 секунд (7 дней). |
| **off-link** | (Опционально.) Укажите, чтобы отключить флаг наличия соединения on-link. Если значение не задано, по умолчанию устанавливается флаг off-link. |
| **no-autoconfig** | (Опционально.) Укажите, чтобы отключить флаг auto-configure. Если значение не задано, флаг auto-configure включается по умолчанию. |

**По умолчанию**

Нет.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Статус префикса представлен следующими комбинациями:

- Комбинация 1: Опции off-link и no-autoconfig не заданы.
  - Префикс добавляется в таблицу маршрутизации. Бит L = 1, бит A = 1.
- Комбинация 2: Задана опция no-autoconfig.
  - Префикс добавляется в таблицу маршрутизации. Бит L = 1, бит A = 0.
- Комбинация 3: Задана опция off-link.
  - Префикс не добавляется в таблицу маршрутизации. Бит L = 0, бит A = 1.

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

**Пример**

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

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 nd prefix 3ffe:501:ffff:100::/64 30000 20000
Switch(config-if)#
```

## *9.12. ipv6 nd ra interval*

Данная команда используется для настройки временного интервала между сообщениями RA для IPv6-интерфейса. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**ipv6 nd ra interval** *MAX-SECS* **[***MIN-SECS***]**

**no ipv6 nd ra interval**

**Параметры**

| | |
|---|---|
| *MAX-SECS* | Укажите максимальный временной интервал для повторной передачи сообщения RA в секундах. Допустимые значения – от 4 до 1800 секунд. |
| *MIN-SECS* | (Опционально) Укажите минимальный временной интервал для повторной передачи сообщения RA в секундах. Данное значение должно быть меньше 75% от максимального значения. Допустимые значения – от 3 до 1350 секунд. |

**По умолчанию**

Максимальный временной интервал по умолчанию – 200 секунд.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Минимальный временной интервал не может быть меньше 3 секунд.

**Пример**

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

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 nd ra interval 1500 1000
Switch(config-if)#
```

## *9.13. ipv6 nd ra lifetime*

Данная команда используется для настройки значения времени жизни (Lifetime) в анонсируемых сообщениях RA. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**ipv6 nd ra lifetime** *SECONDS*

**no ipv6 nd ra lifetime**

**Параметры**

| | |
|---|---|
| *SECONDS* | Укажите продолжительность использования маршрутизатора в качестве маршрутизатора по умолчанию (в секундах). Допустимые значения – от 0 до 9000. |

**По умолчанию**

Значение по умолчанию – 1800 секунд.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

В данном примере показано, как задать значение Lifetime в анонсируемых сообщениях RA.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 nd ra lifetime 9000
Switch(config-if)#
```

## *9.14. ipv6 nd suppress-ra*

Данная команда используется для отключения отправки сообщений RA на интерфейсе. Для включения отправки сообщений RA используйте форму **no**.

**ipv6 nd suppress-ra**

**no ipv6 nd suppress-ra**

**Параметры**

Нет.

**По умолчанию**

Анонсирование RA на интерфейсе VLAN отключено.

Анонсирование RA на интерфейсе туннеля отключено.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте команду **ipv6 nd suppress-ra**, чтобы отключить отправку сообщений RA на интерфейсе. Используйте команду **no ipv6 nd suppress-ra**, чтобы включить отправку сообщений RA на интерфейсе туннеля ISATAP.

**Пример**

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

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 nd suppress-ra
Switch(config-if)#
```

## *9.15. ipv6 nd reachable-time*

Данная команда используется для настройки параметра Reachable Time (время доступности) в таблице ND-протокола. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**ipv6 nd reachable-time** *MILLI-SECONDS*

**no ipv6 nd reachable-time**

**Параметры**

| | |
|---|---|
| *MILLI-SECONDS* | Укажите время доступности для отправляемых анонсов маршрутизатора (в миллисекундах). Допустимые значения – от 0 до 3 600 000, кратно 1000. |

**По умолчанию**

Значение по умолчанию, анонсируемое в сообщениях RA, – 1 200 000.

Значение по умолчанию, используемое маршрутизатором, – 1 200 000 (1200 секунд).

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Заданное время используется маршрутизатором на интерфейсе и анонсируется в сообщении RA. Если задан 0, маршрутизатор будет использовать 1200 секунд на интерфейсе и анонсировать 1200 (не указано) в сообщении RA.

Параметр Reachable Time используется IPv6-узлом для определения доступности соседних узлов.

**Пример**

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

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch (config-if)# ipv6 nd reachable-time 3600000
Switch (config-if)#
```

## *9.16. ipv6 nd ns-interval*

Данная команда используется для настройки временного интервала между повторными отправками сообщений NS. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**ipv6 nd ns-interval** *MILLI-SECONDS*

**no ipv6 nd ns-interval**

**Параметры**

| | |
|---|---|
| *MILLI-SECONDS* | Укажите временной интервал между отправками запросов NS (в миллисекундах). Допустимые значения – от 0 до 3 600 000 миллисекунд, кратно 1000. |

**По умолчанию**

Значение по умолчанию, анонсируемое в сообщениях RA, – 0.

Значение по умолчанию, используемое маршрутизатором, – 1000 (1 секунда).

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

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

**Пример**

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

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch (config-if)# ipv6 nd ns-interval 6000
Switch (config-if)#
```

## *9.17. ipv6 neighbor*

Данная команда используется для создания статической записи в таблице IPv6 neighbor. Используйте форму **no**, чтобы удалить статическую запись из таблицы.

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

**Параметры**

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

**По умолчанию**
Нет.

**Режим ввода команды**
Global Configuration Mode.

**Уровень команды по умолчанию**
Уровень 12.

**Использование команды**
Используйте данную команду для создания статической записи в таблице IPv6 neighbor cache на интерфейсе. Статическая запись будет находиться либо в состоянии REACHABLE, если интерфейс активирован, либо в состоянии INCOMPLETE, если интерфейс выключен. Отслеживание достижимости соседних узлов к статическим записям не применяется.
Команда **clear ipv6 neighbors** позволяет 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)#
```

## *9.18. show ipv6 general-prefix*

Данная команда используется для просмотра информации по основному IPv6-префиксу.

**show ipv6 general-prefix [***PREFIX-NAME***]**

**Параметры**

| | |
|---|---|
| *PREFIX-NAME* | (Опционально) Укажите имя основного префикса, для которого необходимо отобразить информацию. Если имя основного префикса не указано, будет отображаться информация по всем основным префиксам. Имя префикса не должно превышать 12 символов. |

**По умолчанию**
Нет.

**Режим ввода команды**
User EXEC Mode.
Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Используйте данную команду для просмотра информации по основным IPv6-префиксам.

**Пример**

В данном примере показано, как отобразить информацию по всем основным IPv6-префиксам.

```
Switch# show ipv6 general-prefix

IPv6 prefix yy
 Acquired via DHCPv6 PD
   vlan1: 200::/48
       Valid lifetime 2592000, preferred lifetime 604800
   Apply to interfaces
     vlan2: ::2/64

Total Entries: 1

Switch#
```

## *9.19. 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 которого необходимо получить информацию. |
| **brief** | (Опционально.) Укажите, чтобы получить краткую информацию. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode

Любой режим конфигурирования

**Уровень команды по умолчанию**

Уровень 1

**Использование команды**

Используйте данную команду для просмотра настроек конфигурации IPv6-интерфейса. Для интерфейса IPv6-туннеля будет отображаться только туннель ISATAP.

**Пример**

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

```
Switch# show ipv6 interface vlan2

vlan2 is up, Link status is down
  IPv6 is enabled,
  link-local address:
      FE80::201:1FF:FE02:305
  Global unicast address:
      200::2/64 (DHCPv6 PD)
  IP MTU is 1500 bytes
  RA messages are sent between 66 to 200 seconds
  RA advertised reachable time is 1200000 milliseconds
  RA advertised retransmit interval is 0 milliseconds
  RA advertised life time is 1800 seconds
  RA advertised O flag is OFF, M flag is OFF
  RA advertised prefixes
200::/64
valid lifetime is 2592000,  preferred lifetime is 604800

Switch#
```

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

```
Switch# show ipv6 interface brief

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#
```

## *9.20. show ipv6 neighbors*

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

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

**Параметры**

| | |
|---|---|
| *INTERFACE-ID* | Укажите интерфейс для отображения информации о записях в таблице IPv6 neighbor cache. |
| *IPV6-ADDRESS* | Укажите IPv6-адрес, чтобы получить для него информацию о записях в таблице IPv6 neighbor cache. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

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

**Пример**

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

```
Switch# show ipv6 neighbors

IPv6 Address                            Link-Layer Addr   Interface Type State
--------------------------------------- ----------------- --------- ---- -----
FE80::200:11FF:FE22:3344                00-00-11-22-33-44 vlan1     D   REACH

Total Entries: 1

Switch#
```

**Отображаемые параметры**

| | |
|---|---|
| **Тип записи** | D – динамическая изученная запись.<br>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.<br>**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.<br>**STALE** – состояние, в которое переходит запись, если с момента получения последнего подтверждения прошло больше заданного таймером Reachable Time времени (в миллисекундах).<br>**PROBE** – состояние записи, при котором устройство отправляет сообщение Neighbor Solicitation, чтобы подтвердить достижимость. |

# 10. Команды логирования выполненных команд

## *10.1. command logging enable*

Данная команда используется для включения функции логирования выполненных команд. При использовании формы **no** команда отключит функцию логирования.

**command logging enable**

**no command logging enable**

**Параметры**

Нет.

**По умолчанию**

По умолчанию данная опция отключена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 15.

**Использование команды**

Команды логирования используются для записи команд, успешно выполненных через интерфейс командной строки. В журнале ведется запись введенных команд и информации об учетной записи пользователя, в которой была введена команда. Команды, не изменяющие конфигурацию или работу коммутатора (например, **show**), не записываются. Информация о сохранении и просмотре системного журнала описана в характеристиках sys-log.

**Примечание**: если коммутатор находится в режиме BAT (процедура загрузки, загрузка конфигурационного файла и т.д.), ни одна из команд конфигурации не логируется (не будет записана в журнал).

**Пример**

В данном примере показан процесс включения функции логирования.

```
Switch# configure terminal
Switch(config)# command logging enable
Switch(config)#
```

# 11. Команды CPU Access Control List (ACL)

## *11.1. soft-acl filter-map*

Данная команда используется для создания или изменения программных списков управления доступом (software ACL filter map). При использовании этой команды осуществляется вход в режим Software ACL Filter Map. Используйте форму **no** для удаления программных списков управления доступом.

**soft-acl filter-map** *NAME*

**no soft-acl filter-map** *NAME*

**Параметры**

| | |
|---|---|
| *NAME* | Имя программного списка управления доступом (software ACL filter map). Длина имени не должна превышать 32 символов. |

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте данную команду, чтобы перейти в режим Software ACL Filter Map и создать привязку из нескольких предварительно заданных списков ACL для фильтрации пакетов, получаемых CPU. Можно настроить несколько программных списков управления доступом (software ACL filter map).

**Пример**

В данном примере показано, как создать программный список ACL filter map с именем “cpu_filter”.

```
Switch# configure terminal
Switch(config)# soft-acl filter-map cpu_filter
Switch(config-soft-acl)#
```

## *11.2. match access-group*

Данная команда используется для привязки списка доступа к программному списку управления доступом (software ACL filter map). Используйте форму **no** для удаления привязки.

*SEQUENCE-NUMBER* **match mac access-group** *NAME*

*SEQUENCE-NUMBER* **match ip access-group** *NAME*

*SEQUENCE-NUMBER* **match ipv6 access-group** *NAME*

*SEQUENCE-NUMBER* **match expert access-group** *NAME*

**no match {mac | ip | ipv6 | expert} access-group**

**Параметры**

| | |
|---|---|
| *SEQUENCE-NUMBER* | Порядковый номер соответствующей записи совпадения. Диапазон: от 1 до 65535. Чем меньше номер, тем выше приоритет списка доступа. |
| *NAME* | Указывает имя списка доступа ACL, которое должно совпадать. |

**По умолчанию**

Нет.

**Режим ввода команды**

Software ACL Filter Map Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется для привязки списка доступа к программному списку управления доступом (software ACL filter map). К одному программному списку могут быть привязаны несколько списков доступа, при условии что они относятся к разным типам (expert, MAC, IP и IPv6). В случае привязки списков доступа одинакового типа каждая последующая команда перезаписывает предыдущую.

Порядковые номера определяют приоритет обработки связанного списка доступа в filter map. Список доступа с меньшим порядковым номером обладает более высоким приоритетом. Связанные списки доступа с одинаковым порядковым номером обрабатываются в следующем порядке: список доступа expert, список доступа MAC, список доступа IP, список доступа IPv6.

**Пример**

В данном примере показано, как привязать список доступа IP с именем “cpu-acl” и список доступа MAC с именем mac4001 к программному списку управления доступом (software ACL filter map) “cpu_filter”.

```
Switch# configure terminal
Switch(config)# ip access-list cpu-acl
Switch(config-ip-acl)# permit 10.20.0.0 255.255.0.0
Switch(config-ip-acl)# exit
Switch(config)# mac access-list extended mac4001
Switch(config-mac-ext-acl)# 25 deny host 0013.0049.8272 any
Switch(config-mac-ext-acl)# exit
Switch(config)# soft-acl filter-map cpu_filter
Switch(config-soft-acl)# 2 match ip access-group cpu-acl
Switch(config-soft-acl)# 3 match mac access-group mac4001
Switch(config-soft-acl)#
```

## *11.3. match interface*

Данная команда используется для настройки соответствующих входных интерфейсов (ingress interface). Используйте форму **no** для удаления соответствующих входных интерфейсов.

**match interface** *INTERFACE-ID* **[, | -]**

**no match interface {all |** *INTERFACE-ID* **[, | -]}**

**Параметры**

| | |
|---|---|
| *INTERFACE-ID* | Соответствующий идентификатор интерфейса (Interface ID). Корректными интерфейсами являются физические интерфейсы. |
| **,** | (Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы. |

| | |
|---|---|
| **all** | Указывается в форме **no** этой команды, чтобы удалить все совместимые входные интерфейсы. |

**По умолчанию**

Нет.

**Режим ввода команды**

Software ACL Filter Map Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Программный список управления доступом (software ACL filter map) будет активирован, когда настроен один или несколько совместимых интерфейсов. Если совместимый интерфейс не настроен, программный список не вступит в силу.

Когда пакет принимается CPU, и входной интерфейс настроен в программном списке управления доступом (software ACL filter map), коммутатор будет автоматически выполнять поиск связанных списков доступа соответствующего списка.

Связанный список доступа с наивысшим приоритетом в программном списке будет проверен в первую очередь. При обнаружении совпадения другие списки доступа будут проигнорированы. В противном случае, будет выполняться поиск списка доступа со следующим наивысшим приоритетом и так далее.

Внутри списка доступа используется похожая проверка номеров. Правило с меньшим порядковым номером получает более высокий приоритет. При обнаружении совпадения другие правила будут проигнорированы.

В итоге, если совпадение не обнаружено, пакет будет разрешен, и он может непрерывно обрабатываться другими функциями.

Если действием является ‘permit’, он будет пропущен к другим функциям. Если действием является ‘drop’, пакет будет отброшен.

Другими словами, действие программного списка основано на явно настроенной записи «разрешить/запретить». Пакет разрешен, если он не соответствует какому-либо явно заданному правилу «разрешить» или «запретить».

Интерфейс может принадлежать только одному списку. Если интерфейс настроен для нового программного списка, он будет удален из предыдущего списка.

**Пример**

В данном примере показано, как настроить совместимый интерфейс eth 1/0/1 для программного списка управления доступом (software ACL filter map) “cpu_filter”.

```
Switch# configure terminal
Switch(config)# ip access-list cpu-acl
Switch(config-ip-acl)# permit 10.20.0.0 255.255.0.0
Switch(config-ip-acl)# exit
Switch(config)# mac access-list extended mac4001
Switch(config-mac-ext-acl)# 25 deny host 0013.0049.8272 any
Switch(config-mac-ext-acl)# exit
Switch(config)# soft-acl filter-map cpu_filter
Switch(config-soft-acl)# 2 match ip access-group cpu-acl
Switch(config-soft-acl)# 3 match mac access-group mac4001
Switch(config-soft-acl)# match interface ethernet 1/0/1
Switch(config-soft-acl)#
```

## *11.4. show soft-acl*

Данная команда используется для отображения информации о программных списках управления доступом (software ACL filter map).

**show soft-acl filter-map [***NAME***]**

**Параметры**

| | |
|---|---|
| *NAME* | (Опционально) Указывает имя отображаемого программного списка управления доступом. |

**По умолчанию**

Нет.

**Режим ввода команды**

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Используйте данную команду для отображения указанного программного списка управления доступом (software ACL filter map). Если имя не указано, то будут отображаться все списки.

**Пример**

В данном примере показано, как отобразить программный список управления доступом (software ACL filter map).

```
Switch# show soft-acl filter-map

 Software ACL Filter Map
   cpu_filter:
 Match Access-list(s):
   IP(2): Ext-ip
   MAC(3):mac4001
 Match Ingress Interface(s):
   eth1/0/1

Switch#
```

**Отображаемые параметры**

| | |
|---|---|
| **IP(N)** | Тип списка доступа. Число в скобках означает порядковый номер связанного списка доступа. |

# 12. Команды DHCP Snooping

## *12.1. ip dhcp snooping*

Данная команда используется для глобального включения DHCP Snooping. Используйте форму **no**, чтобы отключить DHCP Snooping.

**ip dhcp snooping**

**no ip dhcp snooping**

**Параметры**

Нет.

**По умолчанию**

По умолчанию опция отключена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Функция DHCP Snooping отслеживает пакеты DHCP, поступающие на недоверенный интерфейс во VLAN, на 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 во 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)#
```

## *12.2. ip dhcp snooping information option allow-untrusted*

Данная команда используется для глобального доступа DHCP-пакетов с Relay Option 82 к недоверенным интерфейсам. Используйте форму **no**, чтобы запретить пакеты с Relay Option 82.

**ip dhcp snooping information option allow-untrusted**

**no ip dhcp snooping information option allow-untrusted**

**Параметры**

Нет.

**По умолчанию**

По умолчанию опция отключена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Функция DHCP Snooping проверяет пакеты DHCP, когда они поступают на порт во VLAN, на 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)#
```

## *12.3. ip dhcp snooping database*

Данная команда используется для настройки хранения записей привязки DHCP Snooping в локальной файловой системе (флеш-карте) или на удаленном узле. При использовании формы **no** команда отключит хранение или вернет настройки по умолчанию.

**ip dhcp snooping database {***URL* **| write-delay** *SECONDS***}**

**no ip dhcp snooping database [write-delay]**

**Параметры**

| | |
|---|---|
| *URL* | Укажите URL в любом из представленных форматов:<br>• ftp://username:password@location:tcpport/filename<br>• tftp://location/filename<br>• flash:/filename |
| **write-delay** *SECONDS* | Укажите время ожидания перед обновлением записи при обнаружении изменений в таблице привязки. Время по умолчанию составляет 300 секунд. Диапазон доступных значений от 60 до 86400. |

**По умолчанию**

По умолчанию URL-адрес агента базы данных не установлен.

Значение времени задержки для записи по умолчанию составляет 300 секунд.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется для хранения записей привязки DHCP в локальной Flash-памяти или на удаленном узле. Используйте следующие методы для хранения записей привязки DHCP:

- **flash:** хранение записей в файле в локальной файловой системе.
- **tftp:** хранение записей на удаленном узле через TFTP.
- **ftp:** хранение записей на удаленном узле через FTP.

**Примечание**: Flash-память включает в себя только внешнюю память, например, USB-накопитель.

Используйте данную команду, чтобы сохранить таблицу привязки DHCP Snooping в коммутаторе стека. Таблица не будет сохранена в отдельных коммутаторах стека.

Время аренды записи (lease time) не будет изменено, и время жизни (live time) продолжит отсчитываться, пока запись существует.

**Пример**

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

```
Switch# configure terminal
Switch(config)# ip dhcp snooping database tftp: //10.0.0.2/store/dhcp-snp-bind
Switch(config)#
```

## *12.4. clear ip dhcp snooping database statistics*

Данная команда используется для удаления статистики таблицы привязки DHCP.

**clear ip dhcp snooping database statistics**

**Параметры**

Нет.

**По умолчанию**

Нет.

Режим ввода команды.

Privileged EXEC Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда позволяет удалить статистику таблицы привязки DHCP.

**Пример**

В данном примере показано, как удалить статистику таблицы привязки DHCP Snooping.

```
Switch# clear ip dhcp snooping database statistics
Switch#
```

## *12.5. clear ip dhcp snooping binding*

Данная команда используется для удаления привязки DHCP.

**clear ip dhcp snooping binding [***MAC-ADDRESS***] [***IP-ADDRESS***] [vlan** *VLAN-ID***] [interface** *INTERFACE-ID***]**

**Параметры**

| | |
|---|---|
| *MAC-ADDRESS* | (Опционально) Укажите MAC-адрес, который необходимо удалить. |
| *IP-ADDRESS* | (Опционально) Укажите IP-адрес, который необходимо удалить. |
| **vlan** *VLAN-ID* | (Опционально) Укажите VLAN ID, который необходимо удалить. |

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Опционально) Укажите интерфейс, который необходимо удалить. |

**По умолчанию**

Нет.

**Режим ввода команды**

Privileged EXEC Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда позволяет удалить запись привязки DHCP, включая заданные вручную записи привязки.

**Пример**

В данном примере показано, как удалить все записи привязки DHCP Snooping.

```
Switch# clear ip dhcp snooping binding
Switch#
```

### *12.6. renew ip dhcp snooping database*

Данная команда используется для обновления таблицы привязки DHCP.

**renew ip dhcp snooping database** *URL*

**Параметры**

| | |
|---|---|
| *URL* | Указывается URL-адрес для загрузки таблицы привязки и добавления в нее записей. |

**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 с URL-адреса и добавления записей в таблицу привязки DHCP Snooping.

**Пример**

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

```
Switch# renew ip dhcp snooping database tftp: //10.0.0.2/store/dhcp-snp-bind
Switch#
```

## *12.7. ip dhcp snooping binding*

Данная команда используется для настройки привязки DHCP Snooping вручную.

**ip dhcp snooping binding** *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **expiry** *SECONDS*

**Параметры**

| | |
|---|---|
| *MAC-ADDRESS* | Укажите MAC-адрес записи, которую необходимо добавить или удалить. |
| **vlan** *VLAN-ID* | Укажите VLAN ID записи, которую необходимо добавить или удалить. |
| *IP-ADDRESS* | Укажите IP-адрес записи, которую необходимо добавить или удалить. |
| *INTERFACE-ID* | Укажите интерфейс (физический порт или port channel), на котором необходимо добавить или удалить запись привязки. |
| **expiry** *SECONDS* | Укажите интервал, по истечении которого привязки станут недействительны. Доступен диапазон значений от 60 до 4294967295 секунд. |

**По умолчанию**

Нет.

**Режим ввода команды**

Privileged EXEC Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется для создания динамической записи DHCP Snooping.

**Пример**

В данном примере показано, как настроить запись DHCP Snooping с IP-адресом 10.1.1.1 и MAC-адресом 00-01-02-03-04-05 для VLAN 2 и порта Ethernet 1/0/10 с expiry time, равным 100 секунд.

```
Switch# ip dhcp snooping binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface ethernet 1/0/10 expiry 100
Switch#
```

В данном примере показано, как отключить запись DHCP Snooping с IP-адресом 10.1.1.1 и MAC-адресом 00-01-02-03-04-05 для VLAN 2 и порта Ethernet 1/0/10.

```
Switch# ip dhcp snooping binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface ethernet 1/0/10
Switch#
```

## *12.8. ip dhcp snooping trust*

Данная команда используется для настройки порта в качестве доверенного интерфейса для DHCP Snooping. При использовании формы **no** команда вернет настройки по умолчанию.

**ip dhcp snooping trust**

**no ip dhcp snooping trust**

**Параметры**

Нет.

**По умолчанию**

По умолчанию данная опция отключена.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда позволяет настроить физический порт и интерфейс 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)#
```

## *12.9. ip dhcp snooping limit entries*

Данная команда используется для настройки количества записей привязки DHCP Snooping, которые может изучить интерфейс. При использовании формы **no** команда сбросит заданное ограничение на количество записей DHCP.

**ip dhcp snooping limit entries {***NUMBER* **| no-limit}**

**no ip dhcp snooping limit entries**

**Параметры**

| | |
|---|---|
| *NUMBER* | Укажите ограничение на количество записей привязок DHCP Snooping на порт. Диапазон допустимых значений – от 0 до 1024. |
| **no-limit** | Укажите, чтобы снять ограничение на количество записей. |

**По умолчанию**

По умолчанию данная опция отключена.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда позволяет настроить физический порт и интерфейс port-channel. Команда действует только на недоверенных интерфейсах. Система перестанет изучать привязки, связанные с портом, если превышено максимальное значение.

**Пример**

В данном примере показано, как установить ограничение на количество привязок для Ethernet 1/0/3. Используется значение 100.

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

## *12.10. ip dhcp snooping limit rate*

Данная команда используется для настройки количества DHCP-сообщений, которые интерфейс сможет получать за секунду. При использовании формы **no** команда сбросит заданное ограничение на получение сообщений DHCP.

**ip dhcp snooping limit rate {***VALUE* **| no-limit}**

**no ip dhcp snooping limit rate**

**Параметры**

| | |
|---|---|
| **rate** *VALUE* | Укажите количество DHCP-сообщений, которое может быть обработано за секунду. Диапазон допустимых значений – от 1 до 300. |
| **no-limit** | Укажите для снятия ограничения скорости. |

**По умолчанию**

По умолчанию данная опция отключена.

**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)#
```

## *12.11. ip dhcp snooping station-move deny*

Данная команда используется для отключения состояния DHCP Snooping Station Move. При использовании формы **no** команда включит состояние DHCP Snooping Roaming.

**ip dhcp snooping station-move deny**

**no ip dhcp snooping station-move deny**

**Параметры**

Нет.

**По умолчанию**

По умолчанию опция включена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

При включении DHCP Snooping Station Move динамическая запись привязки DHCP Snooping с теми же VLAN ID и MAC-адресом на определенном порту может переместиться на другой порт, если обнаружится, что новому процессу DHCP принадлежит тот же VLAN ID и MAC-адрес.

**Пример**

В данном примере показано, как отключить состояние Roaming.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping station-move deny
Switch(config)#
```

## *12.12. ip dhcp snooping verify mac-address*

Данная команда используется для включения проверки MAC-адреса источника DHCP-пакета на соответствие аппаратному адресу клиента. При использовании формы **no** команда отключит проверку MAC-адреса.

**ip dhcp snooping verify mac-address**

**no ip dhcp snooping verify mac-address**

**Параметры**

Нет.

**По умолчанию**

По умолчанию опция включена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Функция DHCP Snooping проверяет DHCP-пакеты, присылаемые на порт во VLAN, на которой

включена функция DHCP Snooping. По умолчанию DHCP Snooping проверяет, совпадает ли MAC-адрес источника в заголовке Ethernet с аппаратным адресом DHCP-клиента, чтобы пройти проверку.

**Пример**

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

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

## *12.13. ip dhcp snooping vlan*

Данная команда используется для включения DHCP Snooping в определенной VLAN или группе VLAN. При использовании формы **no** команда отключит DHCP Snooping во VLAN или группе VLAN.

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

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

**Параметры**

| | |
|---|---|
| **vlan** *VLAN-ID* | Укажите VLAN, в которой необходимо включить или отключить функцию DHCP Snooping. |
| , | (Опционально) Используется для перечисления нескольких VLAN или отделения одного диапазона номеров 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 во 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)#
```

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

```
Switch# configure terminal
Switch(config)# ip dhcp snooping vlan 10,15-18
Switch(config)#
```

## 12.14. 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 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:
10, 15-18
Verification of MAC address is disabled
Information option of allowed on un-trusted interface is disabled

Interface    Trusted    Rate Limit
------------ ---------- ------------
eth1/0/1        no      10
eth1/0/8        no      50
eth1/0/9        yes     no_limit

Switch#
```

## 12.15. show ip dhcp snooping binding

Данная команда используется для отображения привязки DHCP Snooping.

**show ip dhcp snooping binding [***IP-ADDRESS***] [***MAC-ADDRESS***] [vlan** *VLAN-ID***] [interface [***INTERFACE-ID* **[, | -]]]**

**Параметры**

| | |
|---|---|
| *IP-ADDRESS* | (Опционально) Укажите, если необходимо отображать привязки на основе IP-адреса. |

| | |
|---|---|
| *MAC-ADDRESS* | (Опционально) Укажите, если необходимо отображать привязки на основе MAC-адреса. |
| **vlan** *VLAN-ID* | (Опционально) Укажите, если необходимо отображать привязки на основе VLAN. |
| **interface** *INTERFACE-ID* | (Опционально) Укажите, если необходимо отображать привязки на основе идентификатора порта (port ID). |
| **,** | (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 EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для отображения привязки DHCP Snooping.

**Пример**

В данном примере показано, как настроить отображение привязок DHCP Snooping.

```
Switch# show ip dhcp snooping binding

MAC Address        IP Address      Lease(seconds)   Type          VLAN  Interface
------------------ --------------- -------------  -------------- ------ ---------
00-01-02-03-04-05 10.1.1.10        1500           dhcp-snooping   100    eth1/0/5
00-01-02-00-00-05 10.1.1.11        1495           dhcp-snooping   100    eth1/0/5

Total Entries: 2

Switch#
```

В данном примере показано, как настроить отображение привязки DHCP Snooping по IP 10.1.1.1.

```
Switch# show ip dhcp snooping binding 10.1.1.1

MAC Address       IP Address      Lease (seconds)   Type           VLAN   Interface
----------------- --------------- -----------------  -------------- ------ ----------
00-01-02-03-04-05 10.1.1.1        1500              dhcp-snooping  100    eth1/0/5

Total Entries: 1

Switch#
```

В данном примере показано, как настроить отображение привязки DHCP Snooping по IP 10.1.1.11 и MAC 00-01-02-00-00-05.

```
Switch# show ip dhcp snooping binding 10.1.1.11 00-01-02-00-00-05

MAC Address         IP Address   Lease (seconds)     Type          VLAN   Interface
------------------ -------------- ------------------  ------------ ------ -----------
00-01-02-00-00-05 10.1.1.11      1495                dhcp-snooping 100    eth1/0/5

Total Entries: 1

Switch#
```

В данном примере показано, как настроить отображение привязки DHCP Snooping по IP 10.1.1.1 и MAC 00-01-02-03-04-05 во VLAN 100.

```
Switch# show ip dhcp snooping binding 10.1.1.11 00-01-02-00-00-05 vlan 100

MAC Address         IP Address    Lease (seconds)   Type           VLAN   Interface
------------------ --------------- ----------------  -------------- ------ -----------
00-01-02-03-04-05 10.1.1.1        1500              dhcp-snooping  100    eth1/0/5

Total Entries: 1
Switch#
```

В данном примере показано, как настроить отображение привязки DHCP Snooping во VLAN 100.

```
Switch# show ip dhcp snooping binding vlan 100

MAC Address         IP Address    Lease (seconds)    Type           VLAN   Interface
------------------ --------------- -----------------  -------------- ------ -----------
00-01-02-03-04-05 10.1.1.10       1500               dhcp-snooping  100    eth1/0/5
00-01-02-00-00-05 10.1.1.11       1495               dhcp-snooping  100    eth1/0/5

Total Entries: 2

Switch#
```

В данном примере показано, как настроить отображение привязки DHCP Snooping на интерфейсе Ethernet 1/0/5.

```
Switch# show ip dhcp snooping binding interface ethernet 1/0/5

MAC Address         IP Address   Lease (seconds)   Type           VLAN   Interface
------------------ -------------- ----------------  -------------- ------ -----------
00-01-02-03-04-05 10.1.1.10      1500              dhcp-snooping  100    eth1/0/5
00-01-02-00-00-05 10.1.1.11      495               dhcp-snooping  100    eth1/0/5

Total Entries: 2

Switch#
```

**Отображаемые параметры**

| | |
|---|---|
| **MAC Address** | Аппаратный MAC-адрес клиента. |
| **IP Address** | IP-адрес клиента, назначенный DHCP-сервером. |
| **Lease (seconds)** | Время аренды IP-адреса (в секундах). |
| **Type** | Тип привязки, настроенный через интерфейс командной строки или изученный динамически. |

| | |
|---|---|
| **VLAN** | VLAN ID. |
| **Interface** | Интерфейс, подключающийся к узлу DHCP-клиента. |

## *12.16. show ip dhcp snooping database*

Данная команда используется для отображения статистики таблицы привязки DHCP Snooping.

**show ip dhcp snooping database**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для отображения статистики таблицы привязки DHCP Snooping.

**Пример**

В данном примере показано, как включить отображение статистики таблицы привязки DHCP Snooping.

```
Switch# show ip dhcp snooping database

URL: tftp://10.0.0.2/store/dhcp-snp-bind
Write Delay Time: 300 seconds

Last ignored bindings counters :
Binding collisions :     0     Expired    lease    :     0
Invalid interfaces :     0     Unsupported vlans :      0
Parse failures       :    0      Checksum errors    :     0

Switch#
```

**Отображаемые параметры**

| | |
|---|---|
| **Binding Collisions** | Количество записей, создавших коллизии с существующими записями в таблице привязки DHCP Snooping. |
| **Expired leases** | Количество записей с истекшим сроком аренды в таблице привязки DHCP Snooping. |
| **Invalid interfaces** | Количество интерфейсов, получивших сообщение DHCP, но DHCP Snooping для которых не выполняется. |
| **Parse failures** | Количество недопустимых пакетов DHCP. |
| **Checksum errors** | Количество подсчитанных значений контрольной суммы, отличных от сохраненного значения контрольной суммы. |

| | |
|---|---|
| **Unsupported vlans** | Количество записей, для которых VLAN отключена. |

# 13. Команды DHCPv6 Guard

## *13.1. ipv6 dhcp guard policy*

Данная команда используется для создания или изменения политики DHCPv6 Guard. Команда позволяет войти в режим DHCPv6 Guard Configuration Mode. При использовании формы **no** данная команда удалит политику DHCPv6 Guard.

**ipv6 dhcp guard policy** *POLICY-NAME*

**no ipv6 dhcp guard policy**

**Параметры**

| | |
|---|---|
| *POLICY-NAME* | Укажите имя политики DHCPv6 Guard. |

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется для создания или изменения политики DHCPv6 Guard. Команда позволяет войти в режим DHCPv6 Guard Configuration Mode. Политики DHCPv6 Guard могут использоваться для блокировки ответов DHCPv6 и сообщений, приходящих с неавторизованного сервера. Сообщения клиента не блокируются.

После создания политики DHCPv6 Guard используйте команду **ipv6 dhcp guard attach-policy** для применения политики на определенном интерфейсе.

**Пример**

В данном примере показано, как создать политику DHCPv6 Guard.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp guard policy policy1
Switch(config-dhcp-guard)# device-role server
Switch(config-dhcp-guard)# match ipv6 access-list acl1
Switch(config-dhcp-guard)#
```

## *13.2. device-role*

Данная команда используется для определения роли подключенного устройства. При использовании формы **no** данная команда вернет настройки по умолчанию.

**device-role {client | server}**

**no device-role**

**Параметры**

| | |
|---|---|
| **client** | Укажите, чтобы настроить подключенное устройство в качестве клиента DHCPv6. Все сообщения сервера DHCPv6 на этом порту будут отбрасываться. |
| **server** | Укажите, чтобы настроить подключенное устройство в качестве сервера DHCPv6. Все сообщения сервера DHCPv6 на этом порту будут приниматься. |

**По умолчанию**

По умолчанию настроена опция **client**.

**Режим ввода команды**

DHCPv6 Guard Policy Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда позволяет определить роль подключенного устройства. По умолчанию устройство выполняет роль клиента, и все сообщения сервера DHCPv6, приходящие на порт, будут отбрасываться. Если настроить устройство в качестве сервера, сообщения сервера DHCPv6 на данном порту будут разрешены.

**Пример**

В данном примере показано, как создать политику DHCPv6 Guard и настроить устройство в качестве сервера.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp guard policy dhcpguard1
Switch(config-dhcp-guard)# device-role server
Switch(config-dhcp-guard)#
```

## *13.3. match ipv6 access-list*

Данная команда используется для проверки IPv6-адреса источника в сообщениях сервера. При использовании формы **no** данная команда отключит проверку.

**match ipv6 access-list** *IPV6-ACCESS-LIST-NAME*

**no match ipv6 access-list**

**Параметры**

| | |
|---|---|
| *IPV6-ACCESS-LIST-NAME* | Укажите список доступа IPv6, с которым необходимо сверяться. |

**По умолчанию**

По умолчанию опция отключена.

**Режим ввода команды**

DHCPv6 Guard Policy Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется для фильтрации DHCPv6-сообщений сервера на основе IP-адреса источника. Если не настроена команда **match ipv6 access-list,** все сообщения сервера будут игнорироваться. Список доступа настраивается с помощью команды **ipv6 access-list**.

**Пример**

В примере ниже показано, как создать политику DHCPv6 Guard и настроить проверку соответствия адресов IPv6 со списком доступа list1.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp guard policy dhcp_filter1
Switch(config-dhcp-guard)# match ipv6 access-list list1
Switch(config-dhcp-guard)#
```

## *13.4. ipv6 dhcp guard attach-policy*

Данная команда используется для применения политики DHCPv6 Guard Policy на определенном интерфейсе. При использовании формы **no** данная команда удалит привязку.

**ipv6 dhcp guard attach-policy [***POLICY-NAME***]**

**no ipv6 dhcp guard attach-policy**

**Параметры**

| | |
|---|---|
| *POLICY-NAME* | (Опционально) Укажите имя политики DHCPv6 Guard. |

**По умолчанию**

По умолчанию опция отключена.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется для применения политики DHCPv6 Guard на интерфейсе. Политики DHCPv6 Guard используются для блокировки DHCPv6-сообщений сервера или фильтрации сообщений сервера на основе IP-адреса источника. Если имя политики не указано, то политика по умолчанию настроит устройство в качестве клиента.

**Пример**

В данном примере показано, как применить политику DHCPv6 Guard «pol1» для интерфейса Ethernet 1/0/3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ipv6 dhcp guard attach-policy pol1
Switch(config-if)#
```

## *13.5. show ipv6 dhcp guard policy*

Данная команда позволяет отобразить информацию о DHCPv6 Guard.

**show ipv6 dhcp guard policy [***POLICY-NAME***]**

**Параметры**

| | |
|---|---|
| *POLICY-NAME* | (Опционально) Укажите имя политики DHCPv6 Guard. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Если указано определенное имя политики, то отображаться будет информация только для нее. Если имя политики не указано, отображаться будет информация для всех политик.

**Пример**

В данном примере показано, как включить отображение информации для всех политик.

```
Switch# show ipv6 dhcp guard policy

DHCP guard policy: default
   Device Role: DHCP client
   Target: eth1/0/3

DHCP guard policy: test1
   Device Role: DHCP server
   Source Address Match Access List: acl1
   Target: eth1/0/1

Switch#
```

**Отображаемые параметры**

| | |
|---|---|
| **Device Role** | Роль устройства: клиент или сервер. |
| **Target** | Название интерфейса. |
| **Source Address Match Access List** | Список доступа IPv6 указанной политики. |

# 14. Команды предотвращения атак DoS

## *14.1. dos-prevention*

Данная команда используется для включения и настройки механизма предотвращения атак DoS. При использовании формы **no** данная команда вернет настройки по умолчанию.

**dos-prevention** *DOS-ATTACK-TYPE*

**no dos-prevention** *DOS-ATTACK-TYPE*

**Параметры**

| | |
|---|---|
| *DOS-ATTACK-TYPE* | Укажите тип DoS-атаки. |

**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 DoS-атак определенного типа или сразу всех поддерживаемых типов. Механизмы предотвращения атак DoS (сопоставление и принятие мер) являются функциями аппаратного обеспечения.

Если функционал предотвращения DoS-атак включен, и был получен хотя бы один «атакующий» пакет, коммутатор сохранит событие в журнале.

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 порядковый номер 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 порядковый номер 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 реализовать атаку.
- **All:** все вышеперечисленные типы.

**Примечание**: некоторые функции, использующие протокол NTP, могут работать некорректно, если включено предотвращение DoS-атак типа **Blat**, так как они используют один и тот же номер порта.

**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)#
```

## *14.2. show dos-prevention*

Данная команда используется для получения информации о статусе предотвращения атак DoS и соответствующих счетчиках, когда пакеты отброшены.

**show dos-prevention [***DOS-ATTACK-TYPE***]**

**Параметры**

| | |
|---|---|
| *DOS-ATTACK-TYPE* | (Опционально) Укажите тип DoS-атаки, который необходимо отобразить. |

**По умолчанию**

Нет.

**Режим ввода команды**

User 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 получить 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 показан процесс вызова информации о настройках предотвращения атак DoS для атаки Land.

```
Switch# show dos-prevention land

DoS Type    : Land Attack
State        : Enabled

Switch#
```

## *14.3. snmp-server enable traps dos-prevention*

Данная команда используется для отправки SNMP-уведомлений о DoS-атаках. Для отключения отправки SNMP-уведомлений используйте форму **no**.

**snmp-server enable traps dos-prevention**

**no snmp-server enable traps dos-prevention**

**Параметры**

Нет.

**По умолчанию**

По умолчанию данная функция отключена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Если предотвращение атак DoS включено, коммутатор будет записывать в журнал событие каждые пять минут, если какой-либо атакующий пакет будет принят за этот промежуток времени. Используйте данную команду, чтобы включить или отключить отправку уведомлений SNMP для таких событий.

**Пример**

В данном примере показано, как включить отправку трапов для атак DoS.

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

# 15. Команды Dynamic ARP Inspection (DAI)

## *15.1. arp access-list*

Данная команда используется для создания или изменения списка доступа ARP. Команда позволяет войти в режим ARP Access-list Configuration Mode. При использовании формы **no** данная команда удалит список доступа ARP.

**arp access-list** *NAME*

**no arp access-list** *NAME*

**Параметры**

| | |
|---|---|
| *NAME* | Укажите имя списка доступа ARP, который необходимо настроить. Максимальная длина – 32 символа. |

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Имя должно быть уникальным среди всех списков доступа. Имя чувствительно к регистру. В конце списка доступа указан запрет в доступе всем, кого нет в списке разрешений.

**Пример**

В данном примере показано, как настроить список доступа ARP с двумя разрешающими записями.

```
Switch# configure terminal
Switch(config)# arp access-list static-arp-list
Switch(config-arp-nacl)# permit ip 10.20.0.0 0.0.255.255 mac any
Switch(config-arp-nacl)# permit ip 10.30.0.0 0.0.255.255 mac any
Switch(config-arp-nacl)#
```

## *15.2. clear ip arp inspection log*

Данная команда используется для очистки буфера журнала ARP Inspection.

**clear ip arp inspection log**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

Privileged EXEC Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется для очистки буфера журнала ARP Inspection.

**Пример**

В данном примере показано, как очистить журнал ARP Inspection.

```
Switch# clear ip arp inspection log
Switch#
```

## *15.3. clear ip arp inspection statistics*

Данная команда используется для удаления данных статистики Dynamic ARP Inspection.

**clear ip arp inspection statistics {all | vlan** *VLAN-ID* **[, | -]}**

**Параметры**

| | |
|---|---|
| **vlan** *VLAN-ID* | (Опционально) Укажите одну VLAN или диапазон VLAN. |

**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#
```

## *15.4. ip arp inspection filter vlan*

Данная команда используется для назначения списка доступа ARP, который будет использоваться для проверки ARP Inspection на VLAN. При использовании формы **no** команда удалит указанную привязку.

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

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

**Параметры**

| | |
|---|---|
| *ARP-ACL-NAME* | Указывается имя списка управления доступом. Максимальная длина – 32 символа. |
| **vlan** *VLAN-ID* | Укажите VLAN, связанную со списком доступа ARP. |
| **,** | (Опционально) Используется для перечисления нескольких VLAN или отделения одного диапазона номеров VLAN от предыдущего. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Используется для обозначения диапазона номеров VLAN. Пробелы до и после дефиса недопустимы. |

| | |
|---|---|
| **static** | (Опционально) Укажите, чтобы 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 назначения 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 на VLAN, для проверки корректности привязки IP-адреса источника и MAC-адреса источника. Во время проверки произойдет сопоставление адреса привязки и записей таблицы DHCP Snooping. Проверка будет производиться, если данная команда сконфигурирована.

Списки управления доступом ARP (ARP ACL) имеют более высокий приоритет, чем таблица DHCP Snooping. Если пакету явно запрещен доступ списком управления доступа, пакет будет отброшен. Если пакету неявно запрещен доступ, он будет дополнительно сопоставлен с записями 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 к VLAN 10 для DAI.

```
Switch# configure terminal
Switch(config)# ip arp inspection filter static-arp-list vlan 10
Switch(config)#
```

## *15.5. ip arp inspection limit*

Данная команда используется для ограничения скорости входящих ARP-запросов и ответов на интерфейсе. При использовании формы **no** команда вернет настройки по умолчанию.

**ip arp inspection limit {rate** *VALUE* **[burst interval** *SECONDS***] | none}**

**no ip arp inspection limit**

**Параметры**

| | |
|---|---|
| **rate** *VALUE* | Укажите максимальное количество ARP-пакетов в секунду, которое может быть обработано. Доступен диапазон значений от 1 до 150. |
| **burst interval** *SECONDS* | (Опционально) Укажите период времени, в течение которого контролируется скорость поступления ARP-пакетов. Доступен диапазон значений от 1 до 15. Если не указано, значение по умолчанию составляет 1 секунду. |
| **none** | Укажите, чтобы не ограничивать скорость передачи ARP-пакетов. |

**По умолчанию**

Для недоверенных интерфейсов DAI ограничение скорости составляет 15 пакетов в секунду с

интервалом burst interval в 1 секунду.

Для доверенных интерфейсов DAI ограничений нет.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется и для доверенных, и для недоверенных интерфейсов. Если количество ARP-пакетов в секунду превышает заданное ограничение и условия 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)#
```

## *15.6. ip arp inspection log-buffer*

Данная команда используется для настройки параметра буфера журнала ARP Inspection.

**ip arp inspection log-buffer entries** *NUMBER*

**no ip arp inspection log-buffer entries**

**Параметры**

| | |
|---|---|
| *NUMBER* | (Опционально) Укажите количество записей в буфере. Максимальное значение – 1024. |

**По умолчанию**

Значение по умолчанию – 32.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется для настройки максимального количества записей в буфере журнала. Буфер журнала ARP Inspection хранит информацию об ARP-пакетах. Первый пакет, прошедший проверку, будет отправлен в модуль системного журнала (syslog) и записан в буфер журнала проверки. Последующие пакеты из той же сессии не будут отправлены в модуль журнала, если только его запись в буфере журнала не будет удалена. Если буфер журнала полон, но события продолжают поступать, они не будут записаны в журнал. Если пользователь задает размер буфера меньше текущего номера записи, буфер журнала будет очищен автоматически.

**Пример**

В примере ниже показано, как изменить размер буфера на 64.

```
Switch# configure terminal
Switch(config)# ip arp inspection log-buffer entries 64
Switch(config)#
```

## *15.7. ip arp inspection trust*

Данная команда используется для добавления интерфейса в список доверенных при использовании Dynamic ARP Inspection. Команда в форме **no** удаляет интерфейс из списка доверенных.

**ip arp inspection trust**

**no ip arp inspection trust**

**Параметры**

Нет.

**По умолчанию**

По умолчанию данная опция отключена.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Если интерфейс находится в состоянии trust (доверенный), ARP-пакеты, поступающие на интерфейс, не будут проверяться. Если интерфейс находится в состоянии untrusted (недоверенный), ARP-пакеты, поступающие на порт и принадлежащие VLAN, в которой включена проверка, будут проверяться.

**Пример**

В данном примере показано, как добавить порт 1/0/3 в список доверенных интерфейсов при использовании DAI.

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

## *15.8. ip arp inspection validate*

Данная команда используется для назначения дополнительных проверок при ARP Inspection. При использовании формы **no** команда отключит дополнительные проверки.

**ip arp inspection validate [src-mac] [dst-mac] [ip]**

**no ip arp inspection validate [src-mac] [dst-mac] [ip]**

**Параметры**

| | |
|---|---|
| **src-mac** | (Опционально) Для ARP-запросов и ответов проверяется соответствие MAC-адреса источника в заголовке Ethernet MAC-адресу отправителя в ARP-заголовке. |
| **dst-mac** | (Опционально) Для ARP-ответов проверяется соответствие MAC-адреса назначения в заголовке Ethernet MAC-адресу получателя в ARP-заголовке. |
| **ip** | (Опционально) Указывается для проверки содержимого ARP на наличие |

| | |
|---|---|
| | недопустимых и непредвиденных IP-адресов. Укажите для проверки допустимости IP-адреса в заголовке ARP. Проверяются IP-адреса источника во всех ARP-запросах и ответах, а также IP-адрес назначения в ARP-ответе. Пакеты, отправляемые на IP-адреса 0.0.0.0, 255.255.255.255 и все IP-адреса многоадресной рассылки отбрасываются. IP-адреса источника проверяются во всех ARP-запросах и ответах, а IP-адреса назначения проверяются только в ARP-ответах. |

**По умолчанию**

По умолчанию данная опция отключена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется для назначения дополнительных проверок во время Dynamic ARP Inspection. Указанная проверка будет производиться с пакетами, поступающими на недоверенный интерфейс и принадлежащими VLAN, для которых включена функция IP ARP Inspection. Если никакие параметры не указаны, все опции включены или выключены. При использовании формы **no** команда отключит дополнительные типы проверок в зависимости от указанного параметра.

**Пример**

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

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

## *15.9. ip arp inspection vlan*

Данная команда используется для включения Dynamic ARP Inspection на определенных VLAN. При использовании формы **no** команда отключит Dynamic ARP Inspection на VLAN.

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

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

**Параметры**

| | |
|---|---|
| **vlan** *VLAN-ID* | Укажите VLAN, для которой необходимо включить или отключить функцию ARP Inspection. |
| **,** | (Опционально) Используется для перечисления нескольких VLAN или отделения одного диапазона номеров 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**

При включении проверки ARP Inspection для выбранной VLAN будут проверяться ARP-запросы и ARP-ответы, поступающие на недоверенный интерфейс и принадлежащие данной VLAN. Если привязка MAC-адреса источника и IP-адреса источника не разрешена правилами ARP ACL, либо таблицей привязки DHCP Snooping, ARP-пакеты будут отброшены. Помимо проверки привязки адреса, будет осуществляться дополнительная проверка, определяемая командой **ip arp inspection validate**.

**Пример**

В данном примере показано, как включить ARP Inspection на VLAN 2.

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 2
Switch(config)#
```

## *15.10. ip arp inspection vlan logging*

Данная команда используется для управления типом пакетов, которые будут логироваться. При использовании формы **no** команда вернет настройки по умолчанию.

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

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

**Параметры**

| | |
|---|---|
| **vlan** *VLAN-ID* | Укажите VLAN, для которой необходимо включить или отключить функцию управления логированием. |
| **,** | (Опционально) Используется для перечисления нескольких VLAN или отделения одного диапазона номеров VLAN от предыдущего. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы. |
| **acl-match** | Укажите критерии логирования для пакетов, отброшенных или разрешенных на основе совпадения со списком управления доступом (ACL). |
| **acl-match permit** | Укажите для логирования, разрешенного сконфигурированным списком управления доступом (ACL). |
| **acl-match all** | Укажите для логирования, разрешенного или запрещенного сконфигурированным списком управления доступом (ACL). |
| **acl-match none** | Укажите, чтобы отменить логирование пакетов на основе совпадения со списком управления доступом (ACL). |
| **dhcp-bindings** | Укажите критерии логирования для пакетов, отброшенных или разрешенных на основе совпадения с привязкой DHCP. |
| **dhcp-bindings permit** | Укажите для логирования, разрешенного привязкой DHCP. |
| **dhcp-bindings all** | Укажите для логирования, разрешенного или запрещенного привязкой DHCP. |

| | |
|---|---|
| **dhcp-bindings none** | Укажите, чтобы отменить логирование всех пакетов, разрешенных или запрещенных на основе привязки DHCP. |

**По умолчанию**

Все запрещенные и отброшенные пакеты логируются.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте форму **no**, чтобы команда вернула критерии логирования по умолчанию.

**Пример**

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

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

## *15.11. permit | deny (arp access-list)*

Данная команда используется для создания разрешающей ARP-записи. Используйте команду **deny** для создания запрещающей ARP-записи. При использовании формы **no** команда удалит запись.

**{permit | deny} ip {any | host** *SENDER-IP* | *SENDER-IP SENDER-IP-MASK***} mac {any | host** *SENDER-MAC* | *SENDER-MAC SENDER-MAC-MASK***}**

**no {permit | deny} ip {any | host** *SENDER-IP* | *SENDER-IP SENDER-IP-MASK***} mac {any | host** *SENDER-MAC* | *SENDER-MAC SENDER-MAC-MASK***}**

**Параметры**

| | |
|---|---|
| **ip any** | Укажите для сопоставления любого IP-адреса источника. |
| **ip host** *SENDER-IP* | Укажите для сопоставления единственного IP-адреса источника. |
| *SENDER-IP SENDER-IP-MASK* | Укажите для сопоставления группы IP-адресов источника с помощью битовой маски (bitmap). Проверяться будет бит, соответствующий значению бита 1. Формат ввода тот же, что и для IP-адреса. |
| **mac any** | Укажите для сопоставления любого MAC-адреса источника. |
| **mac host** *SENDER-MAC* | Укажите для сопоставления единственного MAC-адреса источника. |
| *SENDER-MAC SENDER-MAC-MASK* | Укажите для сопоставления группы MAC-адресов источника с помощью битовой маски (bitmap). Проверяться будет бит, соответствующий значению бита 1. Формат ввода тот же, что и для MAC-адреса. |

**По умолчанию**

Нет.

**Режим ввода команды**

ARP Access-list Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте опцию **permit any**, чтобы разрешить доступ остальным пакетам, не прошедшим проверку по предыдущим правилам.

**Пример**

В данном примере показано, как настроить список доступа ARP с двумя разрешающими записями.

```
Switch# configure terminal
Switch(config)# arp access-list static-arp-list
Switch(config-arp-nacl)# permit ip 10.20.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)# permit ip 10.30.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)#
```

## *15.12. show ip arp inspection*

Данная команда используется для отображения статуса DAI для указанного диапазона VLAN.

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

**Параметры**

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Опционально) Интерфейс (порт), группа интерфейсов (портов) или все интерфейсы (порты), которые необходимо настроить. |
| **,** | (Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы. |
| **vlan** *VLAN-ID* | (Опционально) Укажите VLAN или группу VLAN. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для отображения статуса DAI для указанного диапазона VLAN.

**Пример**

В примере ниже показано, как включить отображение статистики пакетов, которые были обработаны DAI для VLAN 10.

```
Switch# show ip arp inspection statistics vlan 10

VLAN    Forwarded    Dropped    DHCP Drops   ACL Drops
-----   ---------   ---------   ----------   ---------
10       21546        145261       145261        0
VLAN    DHCP Permits   ACL Permits   Source MAC Failures
-----   ------------   -----------   -------------------
10       21546            0               0
VLAN    Dest MAC Failures   IP Validation Failures
-----   -----------------   ----------------------
10       0                       0

Switch#
```

В данном примере показано, как включить отображение статистики пакетов, которые были обработаны DAI для всех активных VLAN.

```
Switch# show ip arp inspection statistics

VLAN    Forwarded    Dropped    DHCP Drops   ACL Drops
-----   ---------   ---------   ----------   ---------
1        0              0            0              0
2        0              0            0              0
10       21546        145261      145261         0
100      0              0            0              0
200      0              0            0              0
1024     0              0            0              0
VLAN    DHCP Permits   ACL Permits   Source MAC Failures
-----   ------------   -----------   -------------------
1        0                0               0
2        0                0               0
10       21546          0               0
100      0                0               0
200      0                0               0
1024     0                0               0
VLAN    Dest MAC Failures   IP Validation Failures
-----   -----------------   ----------------------
1        0                       0
2        0                       0
10       0                       0
100      0                       0
200      0                       0
1024     0                       0

Switch#
```

**Отображаемые параметры**

| | |
|---|---|
| **VLAN** | VLAN ID, на которой действует ARP Inspection. |
| **Forwarded** | Количество ARP-пакетов, переадресованных ARP Inspection. |

| | |
|---|---|
| **Dropped** | Количество ARP-пакетов, отброшенных ARP Inspection. |
| **DHCP Drops** | Количество ARP-пакетов, отброшенных таблицей DHCP Snooping. |
| **ACL Drops** | Количество ARP-пакетов, отброшенных с помощью правил ARP ACL. |
| **DHCP Permits** | Количество ARP-пакетов, разрешенных таблицей DHCP Snooping. |
| **ACL Permits** | Количество ARP-пакетов, разрешенных правилом ARP ACL. |
| **Source MAC Failures** | Количество ARP-пакетов, не прошедших проверку MAC-адреса источника. |
| **Dest MAC Failures** | Количество ARP-пакетов, не прошедших проверку MAC-адреса назначения. |
| **IP Validation Failures** | Количество ARP-пакетов, не прошедших проверку IP-адреса. |

**Пример**

В данном примере показано, как включить отображение настроек и статуса работы DAI.

```
Switch# show ip arp inspection

Source MAC Validation     : Disabled
Destination MAC Validation: Disabled
IP Address Validation     : Disabled
VLAN   State            ACL Match                              Static ACL
----- -------------  -------------------------------- ----------
10      Enabled         -                                        -
VLAN   ACL Logging DHCP Logging
----- ----------- ----------
10      Deny          Deny

Switch#
```

**Отображаемые параметры**

| | |
|---|---|
| **VLAN** | VLAN ID, на котором действует ARP Inspection. |
| **State** | Состояние настроек ARP Inspection.<br>**Enabled:** ARP Inspection работает.<br>**Disabled:** ARP Inspection не работает. |
| **ACL Match** | Имя указанного списка ARP ACL. |
| **Static ACL** | Настройки статического списка управления доступом (static ACL).<br>**Yes**: статический список управления доступом (static ARP ACL) настроен.<br>**No**: статический список управления доступом (static ARP ACL) не настроен. |
| **ACL logging** | Состояние логирования для пакетов, отброшенных или |

| | |
|---|---|
| | разрешенных правилами списка управления доступом (ACL).<br>**None**: пакеты, подпадающие под правила ACL, не логируются.<br>**Permit**: логирование происходит, если пакеты разрешены настроенным списком управления доступом (ACL).<br>**Deny**: логирование происходит, если пакеты отброшены настроенным списком управления доступом (ACL).<br>**All**: логируются все пакеты, подпадающие под правила ACL. |
| **DHCP Logging** | Состояние логирования для пакетов, отброшенных или разрешенных на основе таблицы привязки DHCP.<br>**None**: пакеты, отброшенные или разрешенные таблицей привязки DHCP, не логируются.<br>**Permit**: логирование происходит, если пакеты разрешены таблицей привязки DHCP.<br>**Deny**: логирование происходит, если пакеты отброшены таблицей привязки DHCP.<br>**All**: пакеты, отброшенные или разрешенные таблицей привязки DHCP, логируются. |

**Пример**

В данном примере показано, как получить информацию о состоянии конкретного интерфейса – Ethernet 1/0/3.

```
Switch# show ip arp inspection interfaces ethernet 1/0/3

Interface   Trust State   Rate(pps)  Burst Interval
---------   -----------   ---------  --------------
eth1/0/3     untrusted     30           5

Switch#
```

В данном примере показано, как получить информацию о состоянии всех настроенных интерфейсах коммутатора.

```
Switch# show ip arp inspection interfaces

Interface   Trust State   Rate(pps)    Burst Interval
---------   -----------   ---------   -------------
eth1/0/1      untrusted    30            1
eth1/0/2      untrusted    30            1
eth1/0/3      untrusted    30            5
eth1/0/5      trusted       None         1
eth1/0/6      untrusted    30            1
eth1/0/7      untrusted    30            1
eth1/0/8      untrusted    30            1

Total Entries: 7

Switch#
```

**Отображаемые параметры**

| | |
|---|---|
| **Interface** | Имя интерфейса, на котором работает ARP Inspection. |

| | |
|---|---|
| **Trust State** | Состояние интерфейса.<br>**trusted:** данный интерфейс является доверенным портом ARP Inspection, все ARP-пакеты разрешены и не будут проходить авторизацию.<br>**untrusted:** данный интерфейс является недоверенным портом ARP Inspection, все ARP-пакеты будут проходить авторизацию. |
| **Rate (pps)** | Верхняя граница количества входящих пакетов, обрабатываемых в секунду. |
| **Burst Interval** | Последовательный интервал в секундах, в течение которого на интерфейсе анализируется скорость поступления ARP-пакетов. |

## *15.13. show ip arp inspection log*

Данная команда используется для отображения буфера лога (журнала) ARP Inspection.

**show ip arp inspection log**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для отображения содержимого буфера журнала ARP Inspection.

**Пример**

В данном примере показано, как включить отображение буфера журнала ARP Inspection.

```
Switch# show ip arp inspection log

Total log buffer size: 64

Interface   VLAN        Sender IP          Sender MAC        Occurrence
---------- --------  -------------  -----------------  --------------------------
eth1/0/1     100       10.20.1.1      00-20-30-40-50-60     1 (2013-12-28 23:08:66)
eth1/0/2     100       10.5.10.16     55-66-20-30-40-50     2 (2013-12-02 00:11:54)
eth1/0/3     100       10.58.2.30     10-22-33-44-50-60     1 (2013-12-30 12:01:38)

Total Entries: 3

Switch#
```

**Отображаемые параметры**

| | |
|---|---|
| **Interface** | Имя интерфейса, на котором производится логирование. |

| | |
|---|---|
| **VLAN** | VLAN, на которой производится логирование. |
| **Sender IP** | IP-адрес источника у логируемого ARP. |
| **Sender MAC** | MAC-адрес источника у логируемого ARP. |
| **Occurence** | Счетчик общего числа записей в логе, а также время последнего логирования. |

# 16. Команды управления интерфейсом

## *16.1. clear counters*

Данная команда используется для сброса счетчиков интерфейса.

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

**Параметры**

| | |
|---|---|
| **all** | Укажите, если необходимо сбросить счетчики для всех интерфейсов. |
| *INTERFACE-ID* | Укажите один или несколько интерфейсов, для которых необходимо сбросить счетчики. Интерфейсами могут выступать физические порты, порт управления OOB, port-channel или интерфейсы VLAN 2-го уровня. |
| **,** | (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**

Команда используется для сброса счетчиков для интерфейса физического порта.

**Пример**

В данном примере показано, как сбросить счетчики для Ethernet 1/0/1.

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

## *16.2 description*

Данная команда используется для добавления описания интерфейса. При использовании формы **no** команда удалит описание.

**description** *STRING*

**no description**

**Параметры**

| | |
|---|---|
| *STRING* | Описание 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)#
```

## *16.3. interface*

Данная команда используется для входа в режим Interface Configuration Mode для одного интерфейса. При использовании формы **no** команда удалит интерфейс.

**interface** *INTERFACE-ID*

**no interface** *INTERFACE-ID*

**Параметры**

| | |
|---|---|
| *INTERFACE-ID* | В качестве ID интерфейса указывается тип и номер интерфейса без пробелов между ними. |

**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. ID интерфейса состоит из типа интерфейса и номера интерфейса без пробелов между ними.

Для обозначения интерфейсов используются следующие ключевые слова:

- **Ethernet** – физический Ethernet-порт коммутатора;
- **L2vlan** – интерфейс VLAN уровня 2 на основе IEEE 802.1Q;
- **L2vc** – интерфейс Virtual Circuit уровня 2;
- **Loopback** – программный интерфейс, который всегда находится в рабочем состоянии;
- **Null** – интерфейс null;
- **Port-channel** – агрегированный интерфейс port-channel;
- **Tunnel** – виртуальный интерфейс, используемый для туннелирования;
- **Vlan** – интерфейс VLAN;
- **mgmt** – интерфейс Ethernet, используемый для управления портом out-of-band.

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

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

Для интерфейса null поддерживается интерфейс null0, который не может быть удален.

Для интерфейсов loopback или tunnel команда **interface** используется для создания нового интерфейса или изменения настроек существующего. При использовании формы **no** команда удалит интерфейс.

Режимы интерфейсов **L2vlan** и **L2vc** используются только для добавления описания к существующим интерфейсам L2VLAN и L2 Virtual circuit. Команды **interface l2vlan** и **interface l2vc** не создают новые интерфейсы, а формы no данных команд не удаляют существующие интерфейсы.

**Пример**

В данном примере показано, как войти в режим Interface Configuration Mode для интерфейса Ethernet 1/0/5.

```
Switch# configure terminal
Switch(config)# interface 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 vlan100
Switch(config-if)#
```

В данном примере показано, как войти в режим Interface Configuration Mode для port-channel 3.

```
Switch# configure terminal
Switch(config)# interface port-channel3
Switch(config-if)#
```

В данном примере показано, как добавить интерфейс loopback2 и войти в режим Interface Configuration Mode.

```
Switch# configure terminal
Switch(config)# interface loopback2
Switch (config-if)#
```

В данном примере показано, как удалить интерфейс loopback2.

```
Switch# configure terminal
Switch(config)# no interface loopback2
Switch (config)#
```

## *16.4. interface range*

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

**interface range** *INTERFACE-ID* **[, | -]**

**Параметры**

| | |
|---|---|
| *INTERFACE-ID* | В качестве ID интерфейса указывается тип и номер интерфейса без пробелов между ними. |

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

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**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 указанного диапазона.

**Пример**

В данном примере показано, как войти в режим Interface Configuration Mode для диапазона портов от 2/0/1 до 2/0/5, а также для порта 3/0/3.

```
Switch# configure terminal
Switch(config)# interface range Ethernet 2/0/1-5, 3/0/3
Switch(config-if-range)#
```

## *16.5. show counters*

Данная команда используется для отображения информации об интерфейсе.

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

**Параметры**

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Опционально) Укажите необходимый интерфейс: физический порт, port-channel или VLAN. Если интерфейс не указан, будут отображаться счетчики для всех интерфейсов. |

**По умолчанию**

Нет.

**Режим ввода команды**

User 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 ethernet 1/0/1

eth1/0/1 counters
 rxHCTotalPkts                    : 0
 txHCTotalPkts                    : 0
 rxHCUnicastPkts                  : 0
 txHCUnicastPkts                  : 0
 rxHCMulticastPkts                : 0
 txHCMulticastPkts                : 0
 rxHCBroadcastPkts                : 0
 txHCBroadcastPkts                : 0
 rxHCOctets                       : 0
 txHCOctets                       : 0
 rxHCPkt64Octets                  : 0
 rxHCPkt65to127Octets             : 0
 rxHCPkt128to255Octets            : 0
 rxHCPkt256to511Octets            : 0
 rxHCPkt512to1023Octets           : 0
 rxHCPkt1024to1518Octets          : 0
 rxHCPkt1519to1522Octets          : 0
 rxHCPkt1519to2047Octets          : 0
 rxHCPkt2048to4095Octets          : 0
 rxHCPkt4096to9216Octets          : 0
 txHCPkt64Octets                  : 0
 txHCPkt65to127Octets             : 0
 txHCPkt128to255Octets            : 0
 txHCPkt256to511Octets            : 0
 txHCPkt512to1023Octets           : 0
 txHCPkt1024to1518Octets          : 0
 txHCPkt1519to1522Octets          : 0
 txHCPkt1519to2047Octets          : 0
 txHCPkt2048to4095Octets          : 0
 txHCPkt4096to9216Octets          : 0

 rxCRCAlignErrors                 : 0
 rxUndersizedPkts                 : 0
 rxOversizedPkts                  : 0
 rxFragmentPkts                   : 0
 rxJabbers                        : 0
 rxSymbolErrors                   : 0
 rxDropPkts                       : 0

 txCollisions                     : 0
 ifInErrors                       : 0
 ifOutErrors                      : 0
 ifInDiscards                     : 0
 ifInUnknownProtos                : 0
 ifOutDiscards                    : 0
 txDelayExceededDiscards          : 0
 txCRC                            : 0
```

```
dot3StatsAlignmentErrors           : 0
dot3StatsFCSErrors                 : 0
dot3StatsSingleColFrames           : 0
dot3StatsMultiColFrames            : 0
dot3StatsSQETestErrors             : 0
dot3StatsDeferredTransmisions      : 0
dot3StatsLateCollisions            : 0
dot3StatsExcessiveCollisions       : 0
dot3StatsInternalMacTransmitErrors : 0
dot3StatsCarrierSenseErrors        : 0
dot3StatsFrameTooLongs             : 0
dot3StatsInternalMacReceiveErrors  : 0

linkChange                         : 0

Switch#
```

## *16.6. show interfaces*

Данная команда используется для просмотра информации об интерфейсах.

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

**Параметры**

| | |
|---|---|
| *INTERFACE-ID* | (Опционально) Укажите физический порт, VLAN, интерфейс loopback или другой интерфейс. |
| **,** | (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 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 получить информацию об интерфейсе VLAN для интерфейса VLAN 1.

```
Switch# show interfaces vlan1

VLAN1 is enabled, link status is down
Interface type: VLAN
Interface description: VLAN 1 for MIS
MAC address: 08-00-01-22-00-00

Switch#
```

В данном примере показано, как включить отображение информации об интерфейсе loopback для интерфейса loopback 1.

```
Switch# show interfaces loopback1

loopback1 is enabled, link status is up
Interface type: Loopback
Interface description: Loopback 1 for MIS

Switch#
```

В данном примере показано, как включить отображение информации об интерфейсе NULL для интерфейса null0.

```
Switch# show interfaces null0

Null0 is enabled, link status is up
Interface type: Null
Interface description: Null0 for MIS

Switch#
```

В данном примере показано, как включить отображение информации об интерфейсе для Ethernet 1/0/1.

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

eth1/0/1 is enabled, link status is up
  Interface type: 1000BaseTx
  Interface description: Physical Ethernet port 1/0/1
  MAC Address: 00-03-04-29-00-00
  Auto-duplex, auto-speed, auto-mdix
  Send flow-control: on, receive flow-control: on
  Send flow-control oper: on, receive flow-control oper: on
  Full-duplex, 1Gb/s
  Maximum transmit unit:1536 bytes
  RX rate: 0 bytes/sec, TX rate: 0 bytes/sec
  RX bytes: 0, TX bytes: 0
  RX rate: 0 packets/sec, TX rate: 0
  RX packets: 0, TX packets: 0
  RX multicast: 0, RX broadcast: 0
  RX CRC error: 0, RX undersize: 0
  RX oversize: 0, RX fragment: 0
  RX jabber: 0, RX dropped Pkts: 0
  RX MTU exceeded: 0
  TX CRC error: 0, TX excessive deferral: 0
  TX single collision: 0, TX excessive collision: 0
  TX Late collision: 0, TX collision: 0
```

```
Switch#
```

В данном примере показано, как посмотреть информацию об интерфейсе для порта управления (management port 0).

```
Switch# show interfaces mgmt 0

mgmt0 is enabled, link status is up
Interface type: Management port
Interface description: mgmt_ipif for MIS

Switch#
```

## *16.7. show interfaces counters*

Данная команда используется для отображения счетчиков определенных интерфейсов.

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

**Параметры**

| | |
|---|---|
| *INTERFACE-ID* | (Опционально) Укажите интерфейс: физический порт или интерфейс VLAN. Если интерфейс не указан, отображаться будут счетчики для всех интерфейсов. |
| **,** | (Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы. |
| **errors** | (Опционально) Укажите для отображения счетчика ошибок. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для отображения общих счетчиков, счетчиков ошибок или архивной информации для указанного или всех интерфейсов.

**Пример**

В данном примере показано, как включить отображение счетчиков принятых пакетов (RX) для портов 1 – 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 примере ниже показано, как включить отображение счетчиков ошибок на портах коммутатора.

```
Switch# show interfaces ethernet 1/0/1-8,1/0/14 counters errors

Port      Align-Err   Fcs-Err  Rcv-Err   Undersize  Xmit-Err  OutDiscard
--------- ---------- --------- --------  ---------- --------- -----------
eth1/0/1           0         0         0           0         0           0
eth1/0/2           0         0         0           0         0           0
eth1/0/3           0         0         0           0         0           0
eth1/0/4           0         0         0           0         0           0
eth1/0/5           0         0         0           0         0           0
eth1/0/6           0         0         0           0         0           0
eth1/0/7           0         0         0           0         0           0
eth1/0/8           0         0         0           0         0           0
eth1/0/14          0         0         0           0         0           0

Port          Single-Col Multi-Col  Late-Col    Excess-Col Carri-Sen  Runts
------------- ---------- ---------- ----------  ---------- ---------- ----------

eth1/0/1      0          0          0           0          0          0         0
eth1/0/2      0          0          0           0          0          0         0
eth1/0/3      0          0          0           0          0          0         0
eth1/0/4      0          0          0           0          0          0         0
eth1/0/5      0          0          0           0          0          0         0
eth1/0/6      0          0          0           0          0          0         0
eth1/0/7      0          0          0           0          0          0         0
eth1/0/8      0          0          0           0          0          0         0
eth1/0/14     0          0          0           0          0          0         0

Port          Giants     Symbol-Err SQETest-Err DeferredTx IntMacTx   IntMacRx
------------- ---------- ---------- ----------  ---------- ---------- ----------
eth1/0/1      0          0          0           0          0          0         0
eth1/0/2      0          0          0           0          0          0         0
eth1/0/3      0          0          0           0          0          0         0
eth1/0/4      0          0          0           0          0          0         0
eth1/0/5      0          0          0           0          0          0         0
eth1/0/6      0          0          0           0          0          0         0
eth1/0/7      0          0          0           0          0          0         0
eth1/0/8      0          0          0           0          0          0         0
eth1/0/14     0          0          0           0          0          0         0

Total Entries:12

Switch#
```

## *16.8. show interfaces status*

Данная команда используется для просмотра состояния подключения портов коммутатора.

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

**Параметры**

| | |
|---|---|
| *INTERFACE-ID* | (Опционально) Укажите ID интерфейса. Если интерфейс не указан, отображаться будет состояние подключения всех портов коммутатора. |

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

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для просмотра состояния подключения портов коммутатора.

**Пример**

В примере ниже показано, как посмотреть состояние подключения портов коммутатора.

```
Switch# show interfaces ethernet 1/0/1-8,1/0/14 status

Port          Status        VLAN         Duplex  Speed          Type
------------- ------------- ------------ ------- -------------- -------------
eth1/0/1      not-connected 1            auto    auto           10GBASE-R
eth1/0/2      not-connected 1            auto    auto           10GBASE-R
eth1/0/3      not-connected 1            auto    auto           10GBASE-R
eth1/0/4      not-connected 1            auto    auto           10GBASE-R
eth1/0/5      not-connected 1            auto    auto           10GBASE-R
eth1/0/6      not-connected 1            auto    auto           10GBASE-R
eth1/0/7      connected     trunk        a-full  a-10G          10GBASE-R
eth1/0/8      connected     2            a-full  a-1000         10GBASE-R
eth1/0/14     not-connected 1            auto    auto           10GBASE-R

Total Entries: 10

Switch#
```

## *16.9. show interfaces utilization*

Данная команда используется для просмотра информации о загрузке портов коммутатора.

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

**Параметры**

| | |
|---|---|
| *INTERFACE-ID* | (Опционально) Укажите ID интерфейса. Если параметр не указан, отображаться будет информация о загрузке всех физических портов коммутатора. |
| **,** | (Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до |

| | |
|---|---|
| | и после запятой недопустимы. |
| **-** | (Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы. |
| **utilization** | (Опционально) Укажите для отображения информации о загрузке. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1

**Использование команды**

Команда позволяет пользователю просмотреть информацию о загрузке портов коммутатора.

**Пример**

В примере ниже показано отображение информации о загрузке портов коммутатора.

```
Switch# show interfaces utilization

Port        TX packets/sec  RX packets/sec   Utilization
----------- -------------   --------------   -----------
eth1/0/1      0               0                0
eth1/0/2      1488109         0                50
eth1/0/3      0               0                0
eth1/0/4      0               1488109          50
eth1/0/5      0               0                0
eth1/0/6      0               0                0
eth1/0/7      0               0                0
eth1/0/8      0               0                0

Total Entries: 8

Switch#
```

## *16.10. show interfaces gbic*

Данная команда используется для просмотра информации о состоянии GBIC.

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

**Параметры**

| | |
|---|---|
| *INTERFACE-ID* | (Опционально) Укажите ID интерфейса. Если параметр не указан, отображаться будет информация о состоянии GBIC для всех интерфейсов GBIC. |
| **,** | (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. |
| **gbic** | Отображение информации о состоянии GBIC. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для просмотра информации о состоянии GBIC.

**Пример**

В примере ниже показано отображение информации о состоянии GBIC.

```
Switch# show interfaces gbic

eth1/0/25
 Interface Type: 10GBASE-R
  Laser Identifier: SFP
  Connector Type: LC
   Ethernet Compliance Code: 10G Base-SR
  Encoding: 64B/66B
  Vendor Name: Vendor
  Vendor OUI: 0 :90:65
  Vendor PN: PN1234568790
  Vendor Rev: A2
  Vendor SN: SN1234567890
  Date Code: 110303
  Received Power Measurements Type: Average Power
  Compatibility: Single Mode (SM),10300Mbd, 850nm
  Transfer Distance:
    50/125 um OM2 fiber: 80m
    62.5/125 um OM1 fiber: 30m
     50/125 um OM3 fiber: 300m

eth1/0/26
 Interface type: 10GBASE-R

eth1/1/1
 Interface Type: 40GBASE-SR
```

```
  Laser Identifier: QSFP +
  Extended Identifier: Power Class 1 Module, No CDR in TX, No CDR in RX
  Connector Type: Copper Pigtail
  Ethernet Compliance Code: 40GBASE-CR4
  Encoding: 64B66B
  Vendor Name: Vendor
  Vendor OUI: 0 :18:97
  Vendor PN: PN1234567891
  Vendor Rev: A1
  Vendor SN: SN1234567891
  Date Code: 121009
  Received Power Measurements Type: OMA
  Transmitter Technology: Copper cable unequalized
  Max Case Temp: 70℃
  Compatibility: Single Mode (SM),10400Mbd
  Attenuation At 2.5GHz: 6dB
  Attenuation At 5.0GHz: 9dB
  Transfer Distance:
    copper: 3m

Switch#
```

## *16.11. show interfaces auto-negotiation*

Данная команда используется для просмотра подробной информации об автосогласовании на физических портах.

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

**Параметры**

| | |
|---|---|
| *INTERFACE-ID* | (Опционально) Укажите ID интерфейса. Если параметр не указан, отображаться будет информация обо всех физических портах. |
| **,** | (Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы. |
| **auto-negotiation** | Укажите для отображения подробной информации об автосогласовании. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для просмотра детальной информации об автосогласовании.

**Пример**

В данном примере показано отображение информации об автосогласовании.

```
Switch# show interfaces ethernet 1/1/1-1/1/2 auto-negotiation

eth1/1/1
 Auto Negotiation: Disabled

eth1/1/2
 Auto Negotiation: Enabled

 Remote Signaling: Not detected
 Configure Status: Configuring
 Capability Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
 Capability Advertised Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
 Capability Received Bits: -
 RemoteFaultAdvertised: Disabled
 RemoteFaultReceived: NoError

Switch#
```

## *16.12. show interfaces description*

Данная команда используется для просмотра описания и состояния интерфейсов.

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

**Параметры**

| | |
|---|---|
| *INTERFACE-ID* | (Опционально) Укажите ID интерфейса. Если параметр не указан, отображаться будет 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. |
| **description** | Укажите для отображения описания и состояния интерфейсов. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для просмотра описания и состояния интерфейсов.

**Пример**

В данном примере показано, как посмотреть описание и состояние интерфейсов.

```
Switch#show interfaces description

 Interface              Status    Administrative  Description
 ---------------------  --------  --------------  ------------------------------
 eth1/0/1               up        enabled         Management Department
 eth1/0/2               down      enabled         Sales Department
 eth1/0/3               down      enabled         Branch-1
 eth1/0/4               down      enabled
 eth1/0/5               down      enabled
 eth1/0/6               down      enabled
 eth1/0/7               down      enabled
 eth1/0/8               down      enabled
 eth1/0/9               down      enabled
 eth1/0/10              down      enabled
 eth1/0/11              down      enabled
 eth1/0/12              down      enabled
 eth1/0/13              down      enabled
 eth1/0/14              down      enabled
 eth1/0/15              down      enabled
 eth1/0/16              down      enabled
 eth1/0/17              down      enabled
 eth1/0/18              down      enabled
 eth1/0/19              down      enabled
 eth1/0/20              down      enabled
 eth1/0/21              down      enabled
 eth1/0/22              down      enabled
 eth1/0/23              down      enabled
 eth1/0/24              down      enabled
 mgmt                   down      enabled
 L2VLAN 1               up        enabled
 Interface vlan1        up        enabled

Total Entries:27

Switch#
```

## *16.13. shutdown*

Данная команда используется для отключения интерфейса. При использовании формы **no** команда включит интерфейс.

**shutdown**

**no shutdown**

**Параметры**

Нет.

**По умолчанию**

По умолчанию выбрана опция **no shutdown.**

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда применяется для отключения интерфейсов физического порта, loopback, VLAN, Tunnel и интерфейсов управления. Команда также может использоваться для портов port-channel.

Команда отключает порт. В отключенном состоянии порт не сможет 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
```

# 17. Команды IP Source Guard

## *17.1. ip verify source vlan dhcp-snooping*

Данная команда используется для включения на порту функции защиты IP-адреса – IP Source Guard. При использовании формы **no** команда отключит IP Source Guard.

**ip verify source vlan dhcp-snooping [ip-mac]**

**no ip verify source vlan dhcp-snooping [ip-mac]**

**Параметры**

| | |
|---|---|
| **ip-mac** | (Опционально) Укажите для проверки IP и MAC-адреса получаемых IP-пакетов. |

**По умолчанию**

По умолчанию опция отключена.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Команда используется для настройки физического порта и port-channel. Используйте команду для включения IP Source Guard на необходимом порту.

При включении на порту IP Source Guard IP-пакеты, приходящие на порт, будут проверяться списком управления доступом (ACL). Порт ACL – аппаратный механизм. Его записи могут быть настроены вручную либо получены с помощью таблицы DHCP. Пакет, не прошедший проверку, будет отброшен.

Существует два типа проверки:

- Если **ip-mac** не указан, проверка основана только на IP-адресе источника и VLAN;
- Если **ip-mac** указан, проверка основана на MAC-адресе источника, VLAN и IP-адресе источника.

**Пример**

В данном примере показано, как включить IP Source Guard для Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config-if)#
```

## *17.2. ip source binding*

Данная команда используется для создания статической записи для IP Source Guard. При использовании формы **no** команда удалит статическую запись привязки.

**ip source binding** *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**

**no ip source binding** *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**

**Параметры**

| | |
|---|---|
| *MAC-ADDRESS* | Укажите MAC-адрес для привязки IP-to-MAC. |

| | |
|---|---|
| **vlan** *VLAN-ID* | Укажите VLAN, которой принадлежит проверенный узел. |
| *IP-ADRESS* | Укажите IP-адрес для привязки IP-to-MAC. |
| **interface** *INTERFACE-ID* | Укажите порт, к которому подключен проверенный узел. |
| **,** | (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**

Записей нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте данную команду для создания статической привязки, используемой для проверки IP Source Guard. При использовании формы **no** команда удалит статическую привязку. Указанные параметры команды должны в точности совпадать с настроенными параметрами для удаления.

Если MAC-адрес и VLAN настраиваемой привязки уже есть, существующая привязка будет обновлена. Интерфейсом, указанным для команды, может быть физический порт или port-channel.

**Пример**

В данном примере показано, как настроить привязку IP Source Guard с IP-адресом 10.1.1.1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 на интерфейсе Ethernet 1/0/10.

```
Switch# configure terminal
Switch(config)# ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface ethernet 1/0/10
Switch(config)#
```

В данном примере показано, как удалить привязку IP Source Guard с IP-адресом 10.1.1.1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 на интерфейсе Ethernet 1/0/10.

```
Switch# configure terminal
Switch(config)# no ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface ethernet 1/0/10
Switch(config)#
```

## *17.3. show ip source binding*

Данная команда используется для отображения привязки IP Source Guard.

**show ip source binding [***IP-ADDRESS***] [***MAC-ADDRESS***] [dhcp-snooping | static] [vlan** *VLAN-ID***] [**interface *INTERFACE-ID* **[, | -]]**

**Параметры**

| | |
|---|---|
| *IP-ADDRESS* | (Опционально) Укажите для отображения привязки IP Source Guard на основе IP-адреса. |

| | |
|---|---|
| *MAC-ADDRESS* | (Опционально) Укажите для отображения привязки IP Source Guard на основе MAC-адреса. |
| **dhcp-snooping** | (Опционально) Укажите для отображения привязки IP Source, изученной при помощи DHCP Snooping. |
| **static** | (Опционально) Укажите для отображения привязки IP Source Guard, настроенной вручную. |
| **vlan** *VLAN-ID* | (Опционально) Укажите для отображения привязки IP Source Guard на основе VLAN. |
| *INTERFACE-ID* | (Опционально) Укажите для отображения привязки IP Source Guard на основе порта. |
| **,** | (Опционально) Выделение серии интерфейсов или отделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Записи привязки IP Source Guard либо настраиваются вручную, либо изучаются автоматически с помощью DHCP Snooping для защиты IP-трафика.

**Пример**

В данном примере показано, как настроить отображение привязки IP Source Guard без каких-либо параметров.

```
Switch# show ip source binding

MAC Address       IP Address      Lease(sec)  Type         VLAN   Interface
----------------- --------------- ---------- ------------- ----- -----------
00-01-01-01-01-01 10.1.1.10        infinite  static        100    eth1/0/3
00-01-01-01-01-10 10.1.1.11          3120    dhcp-snooping 100    eth1/0/3

Total Entries: 2

Switch#
```

В данном примере показано, как настроить отображение привязки IP Source Guard для IP-адреса 10.1.1.10.

```
Switch# show ip source binding 10.1.1.10
```

```
MAC Address       IP Address      Lease(sec)  Type         VLAN   Interface
----------------- --------------- ---------- ------------- ----- ----------
00-01-01-01-01-01 10.1.1.10        infinite  static        100    eth1/0/3

Total Entries: 1

Switch#
```

В данном примере показано, как настроить отображение привязки IP Source Guard на основе IP-адреса 10.1.1.11 и MAC-адреса 00-01-01-01-01-10 на VLAN 100 для интерфейса Ethernet 1/0/3, а также задать изучение DHCP Snooping.

```
Switch# show ip source binding 10.1.1.10 00-01-01-01-01-10 dhcp-snooping vlan 100
interface eth1/0/3

MAC Address       IP Address      Lease(sec)  Type         VLAN   Interface
----------------- --------------- ---------- ------------- ----- -----------
00-01-01-01-01-10 10.1.1.11          3564    dhcp-snooping 100    eth1/0/3

Total Entries: 1

Switch#
```

**Отображаемые параметры**

| | |
|---|---|
| **MAC Address** | MAC-адрес клиента. |
| **IP Address** | IP-адрес клиента, назначенный DHCP-сервером или настроенный пользователем. |
| **Lease (sec)** | Время аренды IP-адреса. |
| **Type** | Тип привязки. Статическая привязка настраивается вручную. Динамическая привязка изучается с помощью DHCP Snooping. |
| **VLAN** | Номер VLAN, где находится интерфейс клиента. |
| **Interface** | Интерфейс, подключаемый к узлу DHCP-клиента. |

## *17.4. show ip verify source*

Данная команда используется для отображения записи списка управления доступом (ACL) аппаратного порта на определенном интерфейсе

**show ip verify source [interface** *INTERFACE-ID***] [, | -]]**

**Параметры**

| | |
|---|---|
| *INTERFACE-ID* | (Опционально) Укажите порт или диапазон портов для настройки. |
| **,** | (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 EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для отображения записей в аппаратной таблице ACL.

**Пример**

В данном примере показано, как посмотреть, когда на VLAN 100 – 110 включен DHCP Snooping, на интерфейсе активирован режим IP Source Filter Mode, настроенный как IP, а существующая привязка произведена на основе IP-адреса 10.1.1.1 на VLAN 100.

```
Switch# show ip verify source interface eth1/0/3

Interface  Filter-type  Filter-mode IP address       MAC address       VLAN
---------  -----------  ----------- ---------------  ----------------- -------
eth1/0/3       ip       active      10.1.1.1                           100
eth1/0/3       ip       active      deny-all                           101-120

Total Entries: 2

Switch#
```

В данном примере показано, как посмотреть, что на интерфейсе активирован режим IP Source Filter Mode, настроенный как IP MAC, существующая привязка IP MAC привязывает IP-адрес 10.1.1.10 к MAC-адресу 00-01-01-01-01-01 в VLAN 100 и IP-адрес 10.1.1.11 к MAC-адресу 00-01-01-01-01-10 в VLAN 101.

```
Switch# show ip verify source interface eth1/0/3

Interface  Filter-type  Filter-mode  IP address       MAC address       VLAN
---------  -----------  -----------  ---------------  ----------------- -------
eth1/0/3       ip-mac     active       10.1.1.10        00-01-01-01-01-01 100
eth1/0/3       ip-mac     active       10.1.1.11        00-01-01-01-01-10 101
eth1/0/3       ip-mac     active       deny-all                 -         102-120

Total Entries: 3

Switch#
```

**Отображаемые параметры**

| | |
|---|---|
| **Interface** | Интерфейс, на котором включен IP Inspection. |
| **Filter-type** | Тип действующего IP Source Guard.<br>**ip:** для авторизации IP-пакетов используется только IP-адрес.<br>**ip-mac:** для авторизации IP-пакетов используется IP и MAC-адрес. |

| | |
|---|---|
| **Filter-Mode** | **Active:** активная проверка записей IP Source.<br>**inactive-trust-port:** включить DHCP Snooping для доверенных портов без активной проверки записей IP Source.<br>**inactive-no-snooping-vlan:** не настроено DHCP Snooping в VLAN, нет активной проверки записей IP Source. |
| **IP address** | IP-адрес клиента, назначенный DHCP-сервером или настроенный пользователем. |
| **MAC address** | MAC-адрес клиента. |
| **VLAN** | Номер VLAN интерфейса клиента. |

# 18. Команды IP-MAC-Port Binding (IMPB)

## *18.1. clear ip ip-mac-port-binding violation*

Данная команда используется для удаления заблокированных записей IP-MAC-Port Binding (IMPB).

**clear ip ip-mac-port-binding violation {all | interface** *INTERFACE-ID* **|** *MAC-ADDRESS***}**

**Параметры**

| | |
|---|---|
| **all** | Укажите для удаления всех неразрешенных записей. |
| **interface** *INTERFACE-ID* | Укажите для удаления неразрешенных записей, созданных определенным интерфейсом. |
| *MAC-ADDRESS* | Укажите для удаления неразрешенных записей с определенным MAC-адресом. |

**По умолчанию**

Нет.

**Режим ввода команды**

Privileged EXEC Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Команда используется для удаления неразрешенных записей IMPB из базы данных фильтрации.

**Пример**

В данном примере показано, как удалить заблокированную запись на Ethernet 1/0/4.

```
Switch# clear ip ip-mac-port-binding violation interface ethernet 1/0/4
Switch#
```

## *18.2. ip ip-mac-port-binding*

Данная команда используется для включения управления доступом IMPB для интерфейсов порта. При использовании формы **no** команда отключит функцию управления доступом IMPB.

**ip ip-mac-port-binding [***MODE***]**

**no ip ip-mac-port-binding**

**Параметры**

| | |
|---|---|
| *MODE* | Укажите режим управления доступом IMPB.<br>**strict-mode:** укажите для включения строгого режима управления доступом (strict).<br>**loose-mode:** укажите для включения режима управления доступом loose.<br>Если режим не задан, используется **strict-mode**. |

**По умолчанию**

По умолчанию опция отключена.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Если на порту назначен режим strict-mode, узел может получить доступ к порту только после того, как отправленные им ARP или IP-пакеты пройдут проверку привязок. Чтобы пройти проверку, IP и MAC-адреса источника, VLAN ID и номер порта назначения должны совпадать с любой записью, определенной либо статической привязкой IP Source Guard, либо динамической записью DHCP Snooping.

Если на порту назначен режим loose-mode, узлу будет отказано в доступе к порту, если отправленные им ARP или IP-пакеты не пройдут проверку привязки. Чтобы пройти проверку привязки, IP и MAC-адрес источника, VLAN ID и номер порта назначения должны совпадать с любой записью, определенной либо статической записью привязки IP Source Guard, либо изученной динамической записью DHCP Snooping.

**Пример**

В данном примере показано, как включить управление доступом IMPB на Ethernet 1/0/10.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/10
Switch(config-if)# ip ip-mac-port-binding strict
Switch(config-if)#
```

## *18.3. show ip ip-mac-port-binding*

Данная команда используется для отображения настроек IMPB или записей, заблокированных с помощью функции IMPB.

**show ip ip-mac-port-binding [interface** *INTERFACE-ID* **[, | -]] [violation]**

**Параметры**

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Опционально) Укажите для отображения информации по определенному интерфейсу. |
| **,** | (Опционально) Выделение серии интерфейсов или отделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы. |
| **violation** | (Опционально) Укажите для отображения заблокированной записи. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Используйте данную команду для отображения настроек IMPB или используйте команду **show ip ip-mac-port-binding violation** для отображения записей, заблокированных из-за нарушения проверки IMPB.

**Пример**

В данном примере показано, как включить отображение всех записей, заблокированных функцией IMPB.

```
Switch# show ip ip-mac-port-binding violation

Port       VLAN      MAC Address
------- --------- -------------------
eth1/0/3      1       01-00-0c-cc-cc-cc
eth1/0/3      1       01-80-c2-00-00-00
eth1/0/4      1       01-00-0c-cc-cc-cd
eth1/0/4      1       01-80-c2-00-00-01

Total Entries: 4

Switch#
```

В данном примере показано, как включить отображение настроек IMPB для всех портов.

```
Switch# show ip ip-mac-port-binding

Port           Mode
---------- ------------
eth1/0/1       Strict
eth1/0/2       Strict
eth1/0/3       Loose
eth1/0/4       Loose

Total Entries: 4

Switch#
```

## *18.4. snmp-server enable traps ip-mac-port-binding*

Данная команда используется для включения уведомлений SNMP для функции IP-MAC-Port Binding. При использовании формы **no** команда отключит уведомления SNMP.

**snmp-server enable traps ip-mac-port-binding**

**no snmp-server enable traps ip-mac-port-binding**

**Параметры**

Нет.

**По умолчанию**

По умолчанию данная функция отключена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

При включении данной функции коммутатор будет отправлять трапы о нарушениях безопасности, если будет получен недостоверный пакет. Используйте эту команду для включения или отключения отправки уведомлений SNMP для таких событий.

**Пример**

В данном примере показано, как включить отправку трапов для IP-MAC-Port Binding.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps ip-mac-port-binding
Switch(config)#
```

# 19. Команды IPv6 Snooping

## *19.1 ipv6 snooping policy*

Данная команда используется для создания или изменения политики IPv6 Snooping. Команда позволяет войти в режим IPv6 Snooping Configuration Mode. При использовании формы **no** данная команда удаляет политику IPv6 Snooping.

**ipv6 snooping policy** *POLICY-NAME*

**no ipv6 snooping policy** *POLICY-NAME*

**Параметры**

| | |
|---|---|
| *POLICY-NAME* | Укажите имя политики IPv6 Snooping. |

**По умолчанию**

По умолчанию ни одной политики IPv6 Snooping не создано.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется для создания политики IPv6 Snooping. После создания политики IPv6 Snooping используйте команду **ipv6 snooping attach-policy** для применения политики на указанном интерфейсе.

**Пример**

В данном примере показано, как создать политику IPv6 Snooping с именем policy1.

```
Switch# configure terminal
Switch(config)#ipv6 snooping policy policy1
Switch(config-ipv6-snooping)#
```

### *19.2. protocol*

Данная команда используется для назначения протокола, который будет использоваться для отслеживания адресов, – DHCPv6 или NDP. При использовании формы **no** данная команда отключит использование указанного протокола для IPv6 Snooping.

**protocol {dhcp | ndp}**

**no protocol {dhcp | ndp}**

**Параметры**

| | |
|---|---|
| dhcp | Укажите для отслеживания адресов DHCPv6-пакетов. |
| ndp | Укажите для отслеживания адресов NDP-пакетов. |

**По умолчанию**

По умолчанию все протоколы отключены.

**Режим ввода команды**

IPv6 Snooping Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Функция Neighbor Discovery (ND) Snooping используется для IPv6-адресов, настроенных вручную или созданных с помощью механизма автоконфигурации Stateless Autoconfiguration. Перед назначением IPv6-адреса узел должен сначала выполнить обнаружение Duplicate Address Detection (DAD), позволяющее определить дублирование адресов узлов локальной сети. ND Snooping обнаруживает сообщения DAD, включающие DAD Neighbor Solicitation (NS) и DAD Neighbor Advertisement (NA), для построения таблицы привязки. NDP-пакет (NS и NA) также используется для определения того, доступен ли узел по-прежнему и можно ли удалить привязку или нет.

DHCPv6 Snooping анализирует DHCPv6-пакеты, отправляемые между DHCPv6-клиентом и сервером во время процедуры назначения адреса. Когда DHCPv6-клиент успешно получает действительный IPv6-адрес, DHCPv6 Snooping создает свою таблицу привязок.

**Пример**

В данном примере показано, как включить DHCPv6 Snooping.

```
Switch# configure terminal
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# protocol dhcp
Switch(config-ipv6-snooping)#
```

## *19.3. limit address-count*

Данная команда используется для ограничения максимального количества привязок IPv6 Snooping. При использовании формы **no** данная команда вернет значения по умолчанию.

**limit address-count** *MAXIMUM*

**no limit address-count**

**Параметры**

| | |
|---|---|
| *MAXIMUM* | Укажите максимальное количество привязок IPv6 Snooping. Доступен диапазон значений от 0 до 1024. |

**По умолчанию**

По умолчанию ограничений нет.

**Режим ввода команды**

IPv6 Snooping Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется для ограничения количества привязок IPv6 Snooping, для которых применяется политика IPv6 Snooping. Команда помогает ограничить размер таблицы привязок.

**Пример**

В данном примере показано, как задать максимальное число записей IPv6 Snooping, равное 25.

```
Switch# configure terminal
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# limit address-count 25
Switch(config-ipv6-snooping)#
```

## *19.4. ipv6 snooping attach-policy*

Данная команда используется для применения политики IPv6 Snooping к указанной VLAN. При использовании формы **no** данная команда удалит привязку.

**ipv6 snooping policy attach-policy** *POLICY-NAME*

**no ipv6 snooping policy attach-policy**

**Параметры**

| | |
|---|---|
| *POLICY-NAME* | Укажите имя политики IPv6 Snooping. |

**По умолчанию**

По умолчанию политика IPv6 Snooping не применяется.

**Режим ввода команды**

VLAN Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

После создания политики IPv6 Snooping используйте данную команду для применения политики к определенной VLAN.

**Пример**

В данном примере показано, как включить IPv6 Snooping в VLAN 200.

```
Switch# configure terminal
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# limit address-count 100
Switch(config-ipv6-snooping)# exit
Switch(config)# vlan 200
Switch(config-vlan)# ipv6 snooping attach-policy policy1
Switch(config-vlan)#
```

## *19.5. ipv6 snooping station-move deny*

Данная команда используется для запрета функции Station Move для привязки IPv6 Snooping. При использовании формы **no** данная команда вернет значения по умолчанию.

**ipv6 snooping station-move deny**

**no ipv6 snooping station-move deny**

**Параметры**

Нет.

**По умолчанию**

По умолчанию функция Station Move разрешена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Когда функция Station Move разрешена, динамическая запись привязки Snooping с тем же VLAN ID и MAC-адресом на указанном порту может продвинуться к другому порту, если обнаружены следующие условия:

- Запись привязки DHCPv6 Snooping запускает новый DHCP-процесс на новом интерфейсе;
- Запись привязки ND Snooping запускает новый DAD-процесс на новом интерфейсе.

**Пример**

В данном примере показано, как запретить функцию Station Move.

```
Switch# configure terminal
Switch(config)# ipv6 snooping station-move deny
Switch(config)#
```

## *19.6. show ipv6 snooping policy*

Данная команда используется для просмотра информации о DHCPv6 Guard.

**show ipv6 snooping policy [***POLICY-NAME***]**

**Параметры**

| | |
|---|---|
| *POLICY-NAME* | (Опционально) Укажите имя политики DHCPv6 Guard, которую необходимо отобразить. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для просмотра информации о DHCPv6 Guard. Если параметр не указан, отображаться будет информация для всех политик.

**Пример**

В данном примере показано, как включить отображение информации о DHCPv6 Guard.

```
Switch# show ipv6 snooping policy

Snooping policy: test1
        Protocol: DHCP, NDP
        Limit Address Count: 30
        Target VLAN: 100,200-210,4000

Switch#
```

**Отображаемые параметры**

| | |
|---|---|
| **Protocol** | Протокол, используемый для работы функции обнаружения. |
| **Limit Address Count** | Максимально допустимое число записей для данной политики IPv6 Snooping Policy. |

| | |
|---|---|
| **Target VLAN** | Имя списка VLAN. |

# 20. Команды IPv6 Source Guard

## *20.1. ipv6 source binding vlan*

Данная команда используется для добавления статической записи в таблицу привязки. При использовании формы **no** данная команда удалит статическую привязку.

**ipv6 source binding** *MAC-ADDRESS* **vlan** *VLAN-ID IPV6-ADDRESS* **interface** *INTERFACE-ID*

**no ipv6 source binding** *MAC-ADDRESS* **vlan** *VLAN-ID IPV6-ADDRESS* **interface** *INTERFACE-ID*

**Параметры**

| | |
|---|---|
| *MAC-ADDRESS* | Укажите MAC-адрес привязки, созданной вручную. |
| *VLAN-ID* | Укажите VLAN привязки, созданной вручную. |
| *IPV6-ADDRESS* | Укажите IPv6-адрес привязки, созданной вручную. |
| *INTERFACE-ID* | Укажите номер интерфейса привязки, созданной вручную. |

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется для добавления статической записи в таблицу привязки вручную.

**Пример**

В данном примере показано, как настроить привязку IPv6 Source Guard с IPv6- адресом 2000::1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 на Ethernet 1/0/10.

```
Switch# configure terminal
Switch(config)# ipv6 source binding 00-01-02-03-04-05 vlan 2 2000::1 interface
ethernet 1/0/1
Switch(config)#
```

## *20.2. ipv6 source-guard policy*

Данная команда используется для создания политики IPv6 Source Guard. Команда позволяет войти в режим IPv6 Source-Guard Policy Configuration Mode. При использовании формы **no** данная команда удалит политику IPv6 Source Guard.

**ipv6 source-guard policy** *POLICY-NAME*

**no ipv6 source-guard policy** *POLICY-NAME*

**Параметры**

| | |
|---|---|
| *POLICY-NAME* | Укажите имя политики IPv6 Source Guard. |

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется для создания политики IPv6 Source Guard. Команда позволяет войти в режим IPv6 Source-Guard Policy Configuration Mode.

**Пример**

В данном примере показано, как создать политику IPv6 Source Guard.

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy policy1
Switch(config-source-guard)#
```

## *20.3. deny global-autoconfig*

Данная команда используется для запрета трафика от автоматически сконфигурированных глобальных адресов. При использовании формы **no** команда отключит данную функцию.

**deny global-autoconfig**

**no deny global-autoconfig**

**Параметры**

Нет.

**По умолчанию**

По умолчанию данная опция отключена.

**Режим ввода команды**

Source-Guard Policy Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется для запрета трафика от автоматически сконфигурированных глобальных адресов. Рекомендуется к применению, когда все глобальные адреса назначены DHCP, и администратор хочет заблокировать входящий трафик от узлов с самостоятельно сконфигурированными адресами.

**Пример**

В данном примере показано, как запретить автоматически сконфигурированный трафик.

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy policy1
Switch(config-source-guard)# deny global-autoconfig
Switch(config-source-guard)#
```

## *20.4. permit link-local*

Данная команда используется для аппаратного разрешения трафика данных, отправленных с адреса Link-Local. При использовании формы **no** команда отключит данную функцию.

**permit link-local**

**no permit link-local**

**Параметры**

Нет.

**По умолчанию**

По умолчанию данная опция отключена.

**Режим ввода команды**

Source-Guard Policy Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется для аппаратного разрешения трафика данных, отправленных с адреса Link-Local.

**Пример**

В данном примере показано, как разрешить весь трафик данных, отправленных с адреса Link-Local.

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy policy1
Switch(config-source-guard)# permit link-local
Switch(config-source-guard)#
```

## *20.5. ipv6 source-guard attach-policy*

Данная команда используется для применения IPv6 Source Guard на интерфейсе. При использовании формы **no** данная команда отменит применение IPv6 Source Guard на интерфейсе.

**ipv6 source-guard attach-policy [***POLICY-NAME***]**

**no ipv6 source-guard attach-policy**

**Параметры**

| | |
|---|---|
| *POLICY-NAME* | (Опционально) Укажите имя политики Source Guard. |

**По умолчанию**

Нет.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Когда команда применена к порту, принятый IPv6-пакет, кроме ND, RA, RS и DHCP-сообщений, пройдет проверку привязки адреса. Пакет будет разрешен, если он соответствует любой записи в таблице привязки адресов. Таблица привязки включает в себя динамическую таблицу (созданную с помощью команд IPv6 Snooping) и статическую таблицу (созданную с помощью команды **ipv6 neighbor binding vlan**).

Если имя политики не указано, используется политика Source Guard по умолчанию, которая разрешит пакеты, отправленные с автоматически сконфигурированного адреса, и запретит пакеты, отправленные с адреса Link-Local.

**Пример**

В данном примере показано, как применить политику IPv6 Source Guard «pol1» к Ethernet 1/0/3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ipv6 source-guard attach-policy pol1
Switch(config-if)#
```

## *20.6. show ipv6 source-guard policy*

Данная команда используется для просмотра настроенной политики IPv6 Source Guard.

**show ipv6 source-guard policy [***POLICY-NAME***]**

**Параметры**

| | |
|---|---|
| *POLICY-NAME* | (Опционально) Укажите имя политики Source Guard Policy. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для просмотра настроенной политики IPv6 Source Guard. Если имя политики не указано, отображаться будет информация для всех политик IPv6 Source Guard.

**Пример**

В данном примере показано, как включить отображение настроек для IPv6 Source Guard.

```
Switch# show ipv6 dhcp guard policy

Policy Test configuration:
    permit link-local
    deny global-autoconf
    Target: eth1/0/3

Switch#
```

## *20.7. show ipv6 neighbor binding*

Данная команда используется для просмотра таблицы привязки IPv6.

**show ipv6 neighbor binding [vlan** *VLAN-ID***] [interface** *INTERFACE-ID***] [ipv6** *IPV6-ADDRESS***] [mac** *MAC-ADDRESS***]**

**Параметры**

| | |
|---|---|
| *VLAN-ID* | (Опционально) Укажите для отображения привязок, соответствующих указанной VLAN. |
| *INTERFACE-ID* | (Опционально) Укажите для отображения привязок, соответствующих указанному номеру интерфейса. |
| *IPV6-ADDRESS* | (Опционально) Укажите для отображения привязок, соответствующих указанному IPv6-адресу. |
| *MAC-ADDRESS* | (Опционально) Укажите для отображения привязок, соответствующих указанному MAC-адресу. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Команда используется для просмотра таблицы привязки.

**Пример**

В данном примере показано, как включить отображение указанных записей из таблицы привязки.

```
Switch# show ipv6 neighbor binding

Codes: D - DHCPv6 Snooping, S - Static, N - ND Snooping
  IPv6 address                MAC address     Interface      VLAN Time left
N FE80::A8BB:CCFF:FE01:F500 AABB.CC01.F500 eth1/0/1         100  8850
S FE80::21D:71FF:FE99:4900  001D.7199.4900  eth1/0/2         100   N/A
N 2001:600::1                   AABB.CC01.F500 eth1/0/3          100  3181
D 2001:300::1                   AABB.CC01.F500 port-channel3 100  9559
D 2001:100::2                   AABB.CC01.F600 eth1/0/4          200  9196
D 2001:400::1                   001D.7199.4900 eth1/0/5          100  1568
S 2001:500::1                   000A.000B.000C eth1/0/6         300  N/A

Switch#
```

**Отображаемые параметры**

| | |
|---|---|
| **Codes** | Коды для IPv6 Snooping Owner<br>D: DHCPv6 Snooping<br>S: Статический<br>N: ND Snooping |
| **IPv6 address** | IPv6-адрес привязки. |
| **MAC address** | MAC-адрес привязки. |
| **Interface** | Номер интерфейса привязки. |
| **VLAN** | VLAN привязки. |
| **Time left** | Оставшееся время жизни привязки. Период отсутствия активности для статической привязки. |

# 21. Команды аутентификации MAC

## *21.1. mac-auth system-auth-control*

Данная команда используется для глобального включения MAC-аутентификации. При использовании формы **no** команда отключит глобальную MAC-аутентификацию.

**mac-auth system-auth-control**

**no mac-auth system-auth-control**

**Параметры**

Нет.

**По умолчанию**

По умолчанию данная опция отключена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Функция MAC-аутентификации предназначена для аутентификации пользователей на основе MAC-адреса при попытке доступа к сети через коммутатор. Для аутентификации может использоваться локальная база данных или удаленный RADIUS-сервер.

**Пример**

В данном примере показано, как включить MAC-аутентификацию глобально.

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

## *21.2. mac-auth enable*

Данная команда используется для включения MAC-аутентификации на указанном интерфейсе. При использовании формы **no** команда отключит MAC-аутентификацию.

**mac-auth enable**

**no mac-auth enable**

**Параметры**

Нет.

**По умолчанию**

По умолчанию данная опция отключена.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Команда доступна только для настройки интерфейса физического порта. Она может использоваться для включения MAC-аутентификации на указанном интерфейсе.

Также MAC-аутентификация имеет следующие ограничения:

- MAC-аутентификация на порту не может быть включена, если на данном порту включена функция Port Security.
- MAC-аутентификация на порту не может быть включена, если на данном порту включена функция IP-MAC-Port-Binding.
- MAC-аутентификация не может быть включена на порту, где настроено агрегирование каналов.

**Пример**

В данном примере показано, как включить MAC-аутентификацию на Ethernet 1/0/1.

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

## *21.3. mac-auth password*

Данная команда используется для настройки пароля для локальной и RADIUS-аутентификации. При использовании формы **no** команда вернет значения по умолчанию.

**mac-auth password [0 | 7]** *STRING*

**no mac-auth password**

**Параметры**

| | |
|---|---|
| **0** | (Опционально) Пароль в обычном текстовом виде. Если не указан ни 0, ни 7, по умолчанию пароль будет в обычном текстовом виде. |
| **7** | (Опционально) Зашифрованный пароль. Если не указан ни 0, ни 7, по умолчанию пароль будет в обычном текстовом виде. |
| **password** *STRING* | Укажите, чтобы задать пароль для аутентификации на основе MAC-адреса. Если пароль указан в обычном текстовом виде, длина строки не может превышать 16 символов. |

**По умолчанию**

По умолчанию паролем является MAC-адрес клиента.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Команда используется для настройки пароля, используемого для аутентификации пользователей по MAC-адресу. Если команда не настроена, пароль для аутентификации пользователя по MAC-адресу будет сформирован на основе MAC-адреса. Формат MAC-адреса может быть настроен с помощью команды **authentication mac username format**.

**Пример**

В примере ниже показано, как настроить пароль MAC-аутентификации.

```
Switch# configure terminal
Switch(config)# mac-auth password newpass
Switch(config)#
```

## 21.4. mac-auth username

Данная команда используется для настройки имени пользователя для локальной и RADIUS-аутентификации. При использовании формы **no** команда вернет значения по умолчанию.

**mac-auth username** *STRING*

**no mac-auth username**

**Параметры**

| | |
|---|---|
| username *STRING* | Укажите, чтобы задать имя пользователя для MAC-аутентификации. Длина строки не может превышать 16 символов. |

**По умолчанию**

По умолчанию именем пользователя является MAC-адрес клиента.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Команда предназначена для настройки имени пользователя для аутентификации пользователей по MAC-адресу. Заданное имя пользователя используется для аутентификации через локальную базу данных и удаленные серверы. Если команда не настроена, имя пользователя для аутентификации формируется на основе MAC-адреса.

**Пример**

В данном примере показано, как настроить имя пользователя для аутентификации на основе MAC-адреса.

```
Switch# configure terminal
Switch(config)# mac-auth username user1
Switch(config)#
```

## 21.5. snmp-server enable traps mac-auth

Данная команда используется для включения отправки SNMP-уведомлений для MAC-аутентификации. При использовании формы **no** команда отключит SNMP-уведомления.

**snmp-server enable traps mac-auth**

**no snmp-server enable traps mac-auth**

**Параметры**

Нет.

**По умолчанию**

По умолчанию функция отключена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Нет рекомендаций.

**Пример**

В данном примере показано, как включить отправку трапов для MAC-аутентификации.

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

# 22. Команды Network Access Authentication

## *22.1. authentication guest-vlan*

Данная команда используется для настройки Guest VLAN. При использовании формы **no** команда удалит Guest VLAN.

**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 используется, если указанная VLAN не существует в качестве статической VLAN. Узел не может получить доступ к сети, пока не пройдет аутентификацию. Если настроен Guest VLAN, узлу, не прошедшему аутентификацию, разрешается доступ только к Guest VLAN. Если RADIUS-сервер назначает пользователю VLAN, пользователь будет авторизован в назначенной VLAN. Назначение Guest VLAN и VLAN не действует на порту trunk VLAN и порту 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 останется в Guest VLAN, а PVID порта не будет изменен.

Если Guest VLAN отключена, порт выйдет из Guest VLAN и вернется к Native VLAN. 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)#
```

## *22.2. authentication host-mode*

Данная команда используется для настройки режима аутентификации. При использовании формы **no** команда вернет значения по умолчанию.

**authentication host-mode {multi-host | multi-auth [vlan** *VLAN-ID* **[, | -]]}**

**no authentication host-mode [multi-auth vlan** *VLAN-ID* **[, | -]]**

**Параметры**

| | |
|---|---|
| **multi-host** | Укажите порт для работы в режиме multi-host. Выполняется аутентификация только одного узла, после чего будут разрешены все узлы, подключенные к порту. |
| **multi-auth** | Укажите порт для работы в режиме multi-auth. Каждый узел будет проходить аутентификацию индивидуально. |
| **vlan** *VLAN-ID* | (Опционально) Укажите одну или несколько VLAN аутентификации. Рекомендуется к применению, если для разных VLAN заданы разные требования к аутентификации. При использовании формы **no** будут удалены все VLAN, если не указаны конкретные. В этом случае клиент пройдет аутентификацию, независимо от того, к какой VLAN он принадлежит, даже если его MAC-адрес не аутентифицирован. После успешной аутентификации клиенту не требуется проходить повторную аутентификацию для других VLAN. Данная опция рекомендуется для портов trunk с целью управления аутентификацией на каждой VLAN. Если режим аутентификации порта меняется на multi-host, предыдущие VLAN аутентификации на этом порту будут удалены. |
| **,** | (Опционально) Используется для перечисления нескольких VLAN или отделения одного диапазона номеров 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 режим **multi-auth**.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Если порт работает в режиме **multi-host**, после успешной аутентификации одного из узлов доступ к порту будет разрешен всем остальным узлам. 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, чтобы получить доступ 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)#
```

## *22.3. authentication periodic*

Данная команда используется для включения периодического повторения аутентификации для порта. При использовании формы **no** команда отключит периодическое повторение аутентификации.

**authentication periodic**

**no authentication periodic**

**Параметры**

Нет.

**По умолчанию**

По умолчанию опция отключена.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте команду для включения периодического повторения аутентификации для порта. Используйте команду **authentication timer reauthentication** для настройки таймера повторной аутентификации (re-authentication timer).

**Пример**

В данном примере показано, как включить периодическое повторение аутентификации для порта Ethernet 1/0/1.

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

## *22.4. authentication timer inactivity*

Данная команда используется для настройки таймера бездействия, по истечении которого неактивная сессия будет завершена. При использовании формы **no** команда отключит таймер бездействия.

**authentication timer inactivity {***SECONDS***}**

**no authentication timer inactivity**

**Параметры**

| | |
|---|---|
| *SECONDS* | Укажите период времени в секундах, после которого неактивная сессия будет завершена. Доступен диапазон значений от 120 до 65535. |

**По умолчанию**

По умолчанию опция отключена.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Если таймер бездействия настроен, и сессия пользователя остается неактивной в течение заданного периода времени, такая сессия будет завершена. Значение таймера бездействия (inactivity timer) должно быть меньше значения таймера, настроенного с помощью команды **authentication timer reauthentication**.

**Пример**

В данном примере показано, как настроить значение таймера бездействия на 240 для интерфейса Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication timer inactivity 240
Switch(config-if)#
```

## *22.5. authentication timer reauthentication*

Данная команда используется для настройки таймера, по истечении которого будет необходимо пройти повторную аутентификацию. При использовании формы **no** команда вернет значения по умолчанию.

**authentication timer reauthentication {***SECONDS***}**

**no authentication timer reauthentication**

**Параметры**

| | |
|---|---|
| *SECONDS* | Укажите период времени, по истечении которого будет необходимо пройти повторную аутентификацию. Доступен диапазон значений от 1 до 65535. |

**По умолчанию**

По умолчанию используется значение 3600 секунд.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Команда используется для настройки таймера, по истечении которого необходимо будет 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)#
```

## 22.6. authentication timer restart

Данная команда используется для настройки таймера, по истечении которого станет возможна повторная аутентификация после последней неудачной попытки. При использовании формы **no** команда вернет значения по умолчанию.

**authentication timer restart** *SECONDS*

**no authentication timer restart**

**Параметры**

| | |
|---|---|
| *SECONDS* | Укажите период времени, по истечении которого станет возможна повторная аутентификация. Доступен диапазон значений от 1 до 65535. |

**По умолчанию**

По умолчанию задано 60 секунд.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Коммутатор перейдет в режим молчания (Quiet State) после неудачной попытки аутентификации до истечения времени таймера.

**Пример**

В данном примере показано, как настроить значение таймера повторной аутентификации на 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)#
```

## 22.7. authentication username

Данная команда используется для добавления пользователя в локальную базу данных. При использовании формы **no** команда удалит пользователя из локальной базы данных.

**authentication username** *NAME* **password [0 | 7]** *PASSWORD* **[vlan** *VLAN-ID***]**

**no authentication username** *NAME* **[vlan]**

**Параметры**

| | |
|---|---|
| *NAME* | Укажите имя пользователя (не более 32 символов). |
| **0** | (Опционально) Пароль в обычном текстовом виде. Если не указан ни 0, ни 7, по умолчанию паролем будет обычный текст. |
| **7** | (Опционально) Зашифрованный пароль. Если не указан ни 0, ни 7, по умолчанию паролем будет обычный текст. |

| | |
|---|---|
| **password** *STRING* | Укажите, чтобы задать пароль для MAC-аутентификации. Если указан пароль в обычном текстовом виде, длина строки не должна превышать 32 символов. |
| **vlan** *VLAN-ID* | (Опционально) Укажите, чтобы назначить VLAN. |

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется для настройки локальной базы данных для аутентификации пользователей.

**Пример**

В данном примере показано, как создать учетную запись с именем пользователя user1 и паролем pass1.

```
Switch# configure terminal
Switch(config)# authentication username user1 password pass1
Switch(config)#
```

## *22.8. clear authentication sessions*

Данная команда используется для удаления сессий аутентификации.

**clear authentication sessions {mac | wac | dot1x | all | interface** *INTERFACE-**ID*** **[mac | wac | dot1x] | mac-address** *MAC-ADDRESS***}**

**Параметры**

| | |
|---|---|
| **mac** | Укажите для удаления всех MAC-сессий. |
| **wac** | Укажите для удаления всех WAC-сессий. |
| **dot1x** | Укажите для удаления всех сессий dot1x. |
| **all** | Укажите для удаления всех сессий. |
| **interface** *INTERFACE-ID* | Укажите для удаления сессий порта. |
| **mac-address** *MAC-ADDRESS* | Укажите для удаления сессий определенного пользователя. |

**По умолчанию**

Нет.

**Режим ввода команды**

Privileged EXEC Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Команда используется для удаления сессий аутентификации.

**Пример**

В примере ниже показано, как удалить сессии аутентификации на Ethernet 1/0/1.

```
Switch# clear authentication sessions interface ethernet 1/0/1
Switch#
```

## *22.9. authentication username mac-format*

Данная команда используется для настройки формата MAC-адреса, который будет использоваться в качестве имени пользователя при аутентификации через RADIUS-сервер. При использовании формы **no** команда вернет значения по умолчанию.

**authentication username mac-format case {lowercase | uppercase} delimiter {hyphen | colon | dot | none} number {1 | 2 | 5}**

**no authentication username mac-format**

**Параметры**

| | |
|---|---|
| **lowercase** | Укажите, чтобы использовать символы нижнего регистра. При аутентификации RADIUS имя пользователя будет выглядеть следующим образом: aa-bb-cc-dd-ee-ff |
| **uppercase** | Укажите, чтобы использовать символы верхнего регистра. При аутентификации RADIUS имя пользователя будет выглядеть следующим образом: AA-BB-CC-DD-EE-FF |
| **hyphen** | Укажите, чтобы использовать «-» в качестве разделителя:<br>AA-BB-CC-DD-EE-FF |
| **colon** | Укажите, чтобы использовать «:» в качестве разделителя:<br>AA:BB:CC:DD:EE:FF |
| **dot** | Укажите, чтобы использовать «.» в качестве разделителя:<br>AA.BB.CC.DD.EE.FF |
| **none** | Укажите, чтобы не использовать разделитель:<br>AABBCCDDEEFF |
| **number** | Укажите количество разделителей. Доступны следующие опции:<br>1: один разделитель: AABBCC.DDEEFF<br>2: два разделителя: AABB.CCDD.EEFF<br>5: пять разделителей: AA.BB.CC.DD.EE.FF<br>Если выбран параметр none, разделители не используются. |

**По умолчанию**

По умолчанию в MAC-адресе используются символы верхнего регистра.

По умолчанию в качестве разделителя используется точка.

По умолчанию используется 2 разделителя.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Команда используется для настройки формата имени пользователя на основе MAC-адреса, используемого при аутентификации RADIUS или для IGMP Security.

**Пример**

В данном примере показано, как настроить формат имени пользователя на основе MAC-адреса.

```
Switch# configure terminal
Switch(config)# authentication username mac-format case uppercase delimiter hyphen
number 5
Switch(config)#
```

## *22.10. authentication max users*

Данная команда используется для настройки максимального количества аутентифицированных пользователей для всей системы или для порта. При использовании формы **no** команда вернет значения по умолчанию.

**authentication max users** *NUMBER*

**no authentication max users**

**Параметры**

| | |
|---|---|
| *NUMBER* | Укажите максимальное количество аутентифицированных пользователей. Доступен диапазон значений от 1 до 4096. |

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Команда используется в режимах Global Configuration Mode и Interface Configuration Mode.

Если команда настроена в режиме Global Configuration Mode, задается ограничение на максимальное количество пользователей для всей системы.

Если команда настроена в режиме Interface Configuration Mode, задается ограничение на максимальное количество пользователей для интерфейса.

Данное ограничение задается для пользователей 802.1X, MAC-based Access Control и WAC.

Помимо этого, команда имеет следующее ограничение:

- Если новое значение максимального количества пользователей меньше, чем текущее количество пользователей, команда будет отклонена, и появится сообщение об ошибке.

**Пример**

В данном примере показано, как назначить максимальное количество аутентифицированных

пользователей для системы.

```
Switch# configure terminal
Switch(config)# authentication max users 256
Switch(config)#
```

## *22.11. authentication mac-move deny*

Данная команда используется для запрета MAC move на коммутаторе. При использовании формы **no** команда вернет значения по умолчанию.

**authentication mac-move deny**

**no authentication mac-move deny**

**Параметры**

Нет.

**По умолчанию**

По умолчанию данная опция отключена.

**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. 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, может возникнуть 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 аутнетификации, то узел напрямую может переместиться на него. Сессия с оригинальным портом будет удалена. Аутентифицированный узел можно переместить 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)#
```

## *22.12. authorization disable*

Данная команда используется для отключения приема авторизованной конфигурации. При использовании формы **no** команда включит принятие авторизованной конфигурации.

**authorization disable**

**no authorization disable**

**Параметры**

Нет.

**По умолчанию**

По умолчанию данная опция включена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12

**Использование команды**

Команда используется для включения или отключения принятия авторизованной конфигурации. Если авторизация включена для аутентификации, авторизованные атрибуты (например, VLAN, приоритет 802.1p по умолчанию, Bandwidth (полоса пропускания) и ACL), назначенные RADIUS-сервером, будут приняты, если включено состояние авторизации. Полоса пропускания и список ACL назначаются на основе порта. В режиме multi-auth VLAN и 802.1p назначаются на основе узла.

**Пример**

В данном примере показано, как отключить состояние авторизации.

```
Switch# configure terminal
Switch(config)# no authorization disable
Switch(config)#
```

## *22.13. show authentication sessions*

Данная команда используется для просмотра информации об аутентификации.

**show authentication sessions [mac | wac | dot1x | interface** *INTERFACE-ID* **[, | -] [mac | wac | dot1x] | mac-address** *MAC-ADDRESS***]**

**Параметры**

| | |
|---|---|
| **mac** | (Опционально) Укажите для отображения всех MAC-сессий. |
| **wac** | (Опционально) Укажите для отображения всех WAC-сессий. |
| **dot1x** | (Опционально) Укажите для отображения всех сессий dot1x. |
| **interface** *INTERFACE-ID* | (Опционально) Укажите порт для отображения. |
| **,** | (Опционально) Выделение серии интерфейсов или отделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы. |
| **mac-address** *MAC-ADDRESS* | (Опционально) Укажите для отображения определенного пользователя. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Используйте команду без параметров, чтобы включить отображение сессий со всех портов.

**Пример**

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

```
Switch# show authentication sessions interface ethernet 1/0/1

Interface: eth1/0/1
MAC Address: 00-16-76-35-1A-38
Authentication VLAN: 1
Authentication State: Success
Accounting Session ID: 0000000000CB
Authentication Username: wac
Client IP Address: 10.90.90.9
Aging Time: 3590 sec
Method   State
  WEB-based Access Control: Success, Selected

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.<br>**Start** – узел получен, но аутентификация еще не началась.<br>**Initialization** – источник аутентификации готов, но новая аутентификация не начинается.<br>**Authenticating** – узел проходит аутентификацию.<br>**Failure** – ошибка аутентификации.<br>**Success** – узел прошел аутентификацию. |
| **Accounting Session ID** | Идентификатор сессии учетной записи, который использовался для аккаунтинга после аутентификации. |

| | |
|---|---|
| **Authentication Username** | Имя пользователя узла. Недоступно, пока узел выбран для MAC-Auth. |
| **Client IP Address** | Адрес ассоциированных клиентов. Доступен, только если узел выбран для Web-Auth. |
| **Assigned VID** | Назначенный VLAN ID, разрешенный после прохождения узлом аутентификации. |
| **Assigned Priority** | Назначенный приоритет, разрешенный после прохождения узлом аутентификации. |
| **Assigned Ingress Bandwidth** | Назначенный вход, разрешенный после прохождения узлом аутентификации. |
| **Assigned Egress Bandwidth** | Назначенный выход, разрешенный после прохождения узлом аутентификации. |
| **Method** | Метод аутентификации, например, 802.1X, MAC-Auth, Web-Auth и т.д. |
| **State** | Состояние метода аутентификации.<br>**Authenticating** – узел проходит аутентификацию с помощью данного метода.<br>**Success** – узел успешно прошел аутентификацию с помощью данного метода аутентификации.<br>**Selected** – результат аутентификации данного метода берется и анализируется системой для узла.<br>**Failure** – узел не прошел аутентификацию с помощью данного метода.<br>**No Information** – информация об аутентификации недоступна. |
| **Aging Time/Block Time** | **Aging Time** (время старения) – период времени, в течение которого аутентифицированный узел будет сохраняться в аутентифицированном состоянии. По истечении данного времени узел будет возвращен в не аутентифицированное состояние.<br>**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 заданного периода времени. Доступно только для сессий WEB. |
| **802.1X Authenticator State** | Состояние аутентификатора PAE 802.1X: возможны следующие значения:<br>**INITIALIZE** – аутентификатор в процессе инициализации и ожидает запросов на аутентификацию.<br>**DISCONNECTED** – инициализация завершена, но ни одно запрашивающее устройство не подключено к порту.<br>**CONNECTING** – коммутатор обнаружил, что запрашивающее устройство подключается к порту. PAE произведет попытку установить подключение с запрашивающим устройством.<br>**AUTHENTICATING** – запрашивающее устройство проходит аутентификацию. |

| | |
|---|---|
| | **AUTHENTICATED** – аутентификатор успешно аутентифицировал запрашивающее устройство.<br>**ABORTING** – процедура аутентификации преждевременно отменена из-за получения запроса на повторную авторизацию, кадра EAPOL-Start, кадра EAPOL-Logoff или тайм-айта аутентификации.<br>**HELD** – коммутатор игнорирует или отбрасывает все EAPOL-пакеты для защиты от атак. В данное состояние можно перейти из состояния AUTHENTICATING после ошибки аутентификации.<br>**FORCE_AUTH** – запрашивающее устройство всегда авторизовано.<br>**FORCE_UNAUTH** – запрашивающее устройство всегда не авторизовано. |
| **802.1X Backend State** | Состояние Backend PAE 802.1X. Возможны следующие значения:<br>**REQUEST** – коммутатор получил пакет EAP-запроса от сервера аутентификации и отправил пакет запрашивающему устройству в качестве EAPOL-инкапсулированного кадра.<br>**RESPONSE** – коммутатор получил EAPOL-инкапсулированный пакет EAP-ответа от запрашивающего устройства и отправил EAP-пакет серверу аутентификации.<br>**SUCCESS** – сервер аутентификации подтвердил, что запрашивающее устройство является допустимым клиентом. Backend уведомит аутентификатор PAE и запрашивающее устройство.<br>**FAIL** – сервер аутентификации подтвердил, что запрашивающее устройство является недопустимым клиентом. Backend уведомит конечный автомат аутентификатор PAE и запрашивающее устройство.<br>**TIMEOUT** – на сервере аутентификации или запрашивающем устройстве есть тайм-аут.<br>**IDLE** – коммутатор ожидает начала новой сессии аутентификации.<br>**INITIALIZE** – аутентификатор производит инициализацию. |

# 23. Команды Port Security

## *23.1. clear port-security*

Данная команда позволяет удалить динамически изученные безопасные MAC-адреса.

**clear port-security {all | {address** *MAC-ADDR* **| interface** *INTERFACE-ID* **[, | -]} [vlan** *VLAN-ID***]}**

**Параметры**

| | |
|---|---|
| **all** | Укажите, чтобы удалить все динамически изученные безопасные MAC-адреса. |
| **address** *MAC-ADDR* | Укажите, чтобы удалить указанные динамически изученные безопасные записи на основе введенного MAC-адреса |
| **interface** *INTERFACE-ID* | Укажите, чтобы удалить все динамически изученные безопасные записи на указанном интерфейсе. |
| **,** | (Опционально) Используется для перечисления нескольких интерфейсов или отделения одной группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Используется для обозначения интерфейсов. Пробелы до и после дефиса недопустимы. |
| **vlan** *VLAN-ID* | Укажите, чтобы удалить динамические записи, изученные в указанной VLAN. |

**По умолчанию**

Нет.

**Режим ввода команды**

Privileged EXEC Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Команда позволяет удалить автоматически изученные безопасные MAC-адреса, как динамические, так и постоянные.

**Пример**

В данном примере показано, как удалить определенный безопасный адрес из таблицы MAC-адресов.

```
Switch# clear port-security address 0080.0070.0007
Switch#
```

## *23.2. show port-security*

Данная команда используется для просмотра текущих настроек Port Security.

**show port-security [[interface** *INTERFACE-ID* **[, | -]] [address] | vlan** *VLAN-ID* **[, | -]]**

**Параметры**

| | |
|---|---|
| *INTERFACE-ID* | (Опционально) Укажите ID интерфейса, который необходимо |

| | |
|---|---|
| | отобразить. |
| **,** | (Опционально) Используется для перечисления нескольких интерфейсов или отделения одной группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы. |
| **address** | (Опционально) Укажите для отображения безопасных MAC-адресов, включая настроенные и изученные адреса. |
| **vlan** *VLAN-ID* | (Опционально) Укажите для отображения настроек Port Security для VLAN. |
| **,** | (Опционально) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Укажите диапазон 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**

Команда используется для отображения текущих настроек Port Security.

**Пример**

В данном примере показано, как включить отображение настроек Port Security для Ethernet с 1/0/1 по 1/0/3.

```
Switch# show port-security interface ethernet 1/0/1-3

D:Delete-on-Timeout  P:Permanent
Interface    Max  Curr  Violation     Violation    Security Admin   Current
No.          No.   No.    Act.          Count        Mode   State   State
------------ ---- ---- -------- -------------------- ---- -------- ------------
eth1/0/1     5    2    Restrict          0            D    Enabled  Forwarding
eth1/0/2     10   10   Shutdown          0            D    Enabled  Err-disabled
eth1/0/3     10   0    Shutdown          0            P    Disabled -

Total Entries: 3

Switch#
```

## *23.3. snmp-server enable traps port-security*

Данная команда используется для включения отправки SNMP-уведомлений при обнаружении функционалом Port Security недопустимых адресов. При использовании формы **no** команда отключит отправку SNMP-уведомлений.

**snmp-server enable traps port-security [trap-rate** *TRAP-RATE***]**

**no snmp-server enable traps port-security [trap-rate]**

**Параметры**

| | |
|---|---|
| **trap-rate** *TRAP-RATE* | (Опционально) Укажите количество трапов в секунду. Доступен диапазон значений от 0 до 1000. Значение по умолчанию 0 означает, что SNMP-трап будет генерироваться для каждого нарушения безопасности. |

**По умолчанию**

По умолчанию функция отключена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Нет.

**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)#
```

### *23.4. switchport port-security*

Данная команда используется для настройки параметров Port Security, чтобы ограничить количество пользователей, которым разрешен доступ к порту. Используйте форму **no** этой команды для отключения Port Security или удаления безопасного MAC-адреса.

**switchport port-security [maximum** *VALUE* **| violation {protect | restrict | shutdown} | mode {permanent | delete-on-timeout} | mac-address [permanent]** *MAC-ADDRESS* **[vlan** *VLAN-ID***]]**

**no switchport port-security [maximum | violation | mode | mac-address [permanent]** *MAC-ADDRESS* **[vlan** *VLAN-ID***]]**

**Параметры**

| | |
|---|---|
| **maximum** *VALUE* | (Опционально) Укажите максимальное число разрешенных безопасных MAC-адресов. Если не указано, значение по умолчанию – 32. Доступен диапазон значений от 0 до 12288. |
| **protect** | (Опционально) Укажите, если необходимо отбрасывать все пакеты с незащищенных узлов на уровне port-security без увеличения значений счетчика нарушений безопасности (security-violation). |

| | |
|---|---|
| **restrict** | (Опционально) Укажите, если необходимо отбрасывать все пакеты с незащищенных узлов на уровне port-security с увеличением значений счетчика нарушений безопасности (security-violation) и записью в системный журнал (system log). |
| **Shutdown** | (Опционально) Укажите для отключения порта, если произошло нарушение безопасности, и сохранения события в системный журнал. |
| **permanent** | (Опционально) В данном режиме все изученные MAC-адреса не будут удалены, пока пользователь не удалит их вручную. |
| **delete-on-timeout** | (Опционально) В данном режиме все изученные MAC-адреса будут удалены, когда запись устареет, или если пользователь удалит записи вручную. |
| **mac-address** *MAC-ADDRESS* | (Опционально) Укажите, чтобы добавить безопасный MAC-адрес для получения доступа к порту. |
| **permanent** | (Опционально) Укажите, чтобы задать безопасный постоянно настроенный MAC-адрес порта. Данная запись является такой же, как изученная в режиме Permanent Mode. |
| **vlan** *VLAN-ID* | (Опционально) Укажите VLAN. Если VLAN не указана, MAC-адрес будет изучен в соответствии с PVID. |

**По умолчанию**

По умолчанию опция отключена.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Когда включена функция Port Security и для порта настроен режим **delete-on-timeout**, порт будет автоматически изучать безопасные записи и хранить их, пока не истечет их тайм-аут. Время хранения этих записей зависит от настроек, заданных командой **switchport port-security aging**. Если режим порта задан как постоянный (permanent), он будет автоматически изучать безопасные записи с неистекающим тайм-аутом. Автоматически изученные безопасные записи будут храниться в текущем файле конфигурации (running configuration).

При изменении 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 работать одновременно с 802.1X, MAC-based Access Control (управление доступом на основе MAC), WAC и IMPB, которые предоставляют более широкие возможности управления безопасностью.
- Если порт указан в качестве порта назначения для функции зеркалирования, функция Port Security не может быть включена.
- Если порт указан в качестве порта агрегирования каналов, функция Port Security не может быть включена.

При превышении максимального количества безопасных пользователей может быть предпринято одно из следующих действий:

- **Protect** – когда число безопасных MAC-адресов порта достигает максимального значения пользователей, разрешенного на порту, пакеты с неизвестным адресом источника будут отбрасываться до тех пор, пока какая-нибудь безопасная запись не будет удалена.
- **Restrict** – при нарушении безопасности происходит ограничение данных, и возрастает счетчик нарушений безопасности.
- **Shutdown** – при нарушении безопасности интерфейс отключается на основе ошибок.

**Пример**

В данном примере показано, как настроить режим permanent для Port Security с 5 безопасными MAC-адресами, разрешенными на порту.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security mode permanent
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)#
```

В данном примере показано, как вручную добавить безопасный MAC-адрес 00-00-12-34-56-78 с VID 5 на Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security mac-address 00-00-12-34-56-78 vlan 5
Switch(config-if)#
```

В данном примере показано, как настроить отбрасывание всех пакетов от небезопасных узлов на уровне port-security с увеличением счетчика нарушений при обнаружении нарушений безопасности.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)#
```

## *23.5. switchport port-security aging*

Данная команда позволяет задать время старения для динамически изученных безопасных адресов на интерфейсе. При использовании формы **no** команда вернет значения по умолчанию.

**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. Доступен 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 функция отключена.

Время хранения по умолчанию – 0 минут.

Тип хранения по умолчанию – absolute.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Команда используется для отключения процесса старения записей, а также для того, чтобы задать время старения динамически изученных безопасных записей. Для того чтобы задать тип inactivity, должна быть включена функция FDB table aging.

**Пример**

В данном примере показано, как настроить время старения динамически изученных безопасных MAC-адресов для Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security aging 1
Switch(config-if)#
```

В данном примере показано, как настроить тип времени старения для Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)#
```

## *23.6. port-security limit*

Данная команда позволяет задать максимальное количество безопасных MAC-адресов в системе или на указанной VLAN. При использовании формы **no** команда вернет настройки по умолчанию.

**port-security limit {global | vlan** *VLAN-ID* **[, | -]}** *VALUE*

**no port-security limit {global | vlan** *VLAN-ID* **[, | -]}**

**Параметры**

| | |
|---|---|
| **global** | Укажите, если необходимо применить настройки ко всей системе. |

| | |
|---|---|
| **vlan** *VLAN-ID* | Укажите необходимые VLAN ID. |
| **,** | (Опционально) Используется для перечисления нескольких VLAN или отделения одного диапазона номеров VLAN от предыдущего. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Укажите диапазон VLAN. Пробелы до и после дефиса недопустимы. |
| *VALUE* | Укажите максимальное число записей Port Security, которое может быть изучено в системе или в указанной VLAN. Доступен диапазон значений от 1 до 12288. Если указанное значение меньше текущего числа изученных записей, команда будет отклонена. |

**По умолчанию**

По умолчанию в данной опции ограничений нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда позволяет ограничить количество изученных безопасных MAC-адресов в системе или в VLAN.

**Пример**

В данном примере показано, как настроить максимальное число безопасных MAC-адресов для системы.

```
Switch# configure terminal
Switch(config)# port-security limit global 100
Switch(config)#
```

# 24. Команды Private VLAN

## *24.1. private-vlan*

Данная команда позволяет настроить VLAN в качестве Private VLAN. При использовании формы **no** команда удалит настройки Private VLAN.

**private-vlan {community | isolated | primary}**

**no private-vlan {community | isolated | primary}**

**Параметры**

| | |
|---|---|
| **community** | Укажите для настройки VLAN в качестве общедоступной (Community) в домене Private VLAN. Порты в Community VLAN могут обмениваться информацией друг с другом, но не с портами других Community VLAN на 2 уровне. |
| **isolated** | Укажите для настройки VLAN в качестве изолированной (Isolated) в домене Private VLAN. Порты в Isolated VLAN не могут обмениваться информацией друг с другом и с портами других Community VLAN на 2 уровне. |
| **primary** | Укажите для настройки VLAN в качестве Primary в домене Private VLAN. |

**По умолчанию**

Нет.

**Режим ввода команды**

VLAN Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Частный домен VLAN определяется одной основной (Primary) VLAN, одной изолированной (Isolated) VLAN и несколькими общедоступными (Community) VLAN. Используйте данную команду, чтобы указать роль Private VLAN перед дальнейшей настройкой Private VLAN с помощью других команд.

**Пример**

В данном примере показано, как настроить VLAN в качестве Private VLAN. VLAN 1000, VLAN 1001 и VLAN 1002 настроены в качестве Primary VLAN, Isolated VLAN и Community VLAN соответственно.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 1001
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 1002
Switch(config-vlan)# private-vlan community
Switch(config-vlan)#
```

## *24.2. private-vlan association*

Данная команда позволяет ассоциировать второстепенную VLAN с основной VLAN. При использовании формы **no** команда отменит ассоциирование VLAN.

**private-vlan association {add** *SECONDARY-VLAN-ID* **[, | -] | remove** *SECONDARY-VLAN-ID* **[, | -]}**

**no private-vlan association**

**Параметры**

| | |
|---|---|
| **add** *SECONDARY-VLAN-ID* | Укажите для связи указанной второстепенной VLAN с основной VLAN. |
| **remove** *SECONDARY-VLAN-ID* | Укажите, чтобы удалить связь указанной второстепенной сети VLAN с основной сетью VLAN. |
| **,** | (Опционально) Используется для перечисления нескольких VLAN или отделения одного диапазона номеров VLAN от предыдущего. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Используется для обозначения диапазона номеров VLAN. Пробелы до и после дефиса недопустимы. |

**По умолчанию**

Нет.

**Режим ввода команды**

VLAN Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Только одна Isolated VLAN может быть связана с основной сетью VLAN. Несколько общедоступных (Community) VLAN могут быть связаны с основной (Primary) VLAN. Второстепенная VLAN может быть связана только с одной основной (Primary) VLAN.

**Пример**

В данном примере показано, как связать второстепенную VLAN 1001 и второстепенную VLAN 1002 с основной VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# private-vlan association add 1001-1002
Switch(config-vlan)#
```

## *24.3. private-vlan synchronize*

Данная команда используется для синхронизации второстепенных VLAN, чтобы иметь тот же самый идентификатор сопоставления MST (mapping MST ID), что и основная VLAN.

**private-vlan synchronize**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

MST Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Второстепенные VLAN должны быть сопоставлены с теми же MST ID, что и основная VLAN, если настроена Private VLAN. Если сопоставление не синхронизировано при выходе пользователя из режима MST Configuration Mode, появится предупреждающее сообщение. Используйте команду private-vlan synchronize, чтобы синхронизировать сопоставление MST ID перед выходом из режима MST Configuration Mode. Данная команда не будет сохранена в текущий файл конфигурации (running configuration).

**Пример**

В данном примере показано, как синхронизировать сопоставление MST (MST Mapping) перед выходом из режима MST Configuration Mode.

```
Switch# configure terminal
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlans 1-100
Switch(config-mst)# instance 2 vlans 101-200
Switch(config-mst)# private-vlan synchronize
Switch(config-mst)#
```

## *24.4. switchport mode private-vlan*

Данная команда позволяет назначить порт в качестве порта Private VLAN. Доступные типы порта – Host port (порт узла) и Promiscuous port. При использовании формы **no** команда вернет настройки по умолчанию.

**switchport mode private-vlan {host | promiscuous | trunk promiscuous | trunk secondary}**

**no switchport mode**

**Параметры**

| | |
|---|---|
| **host** | Укажите порт в качестве Isolated port или Community port. |
| **promiscuous** | Укажите порт в качестве Promiscuous port. |
| **trunk promiscuous** | Укажите порт в качестве Trunk Promiscuous port. |
| **trunk secondary** | Укажите порт в качестве Trunk Secondary port. |

**По умолчанию**

По умолчанию данная опция настроена в режиме Hybrid VLAN mode.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Для портов Isolated или Community используйте команду switchport mode private-vlan host, чтобы указать режим порта, и команду switchport private-vlan host-association, чтобы связать порт с второстепенной VLAN и основной VLAN.

Для порта Promiscuous используйте команду **switchport mode private-vlan promiscuous**, чтобы указать режим порта, и команду **switchport private-vlan mapping**, чтобы связать порт с основной VLAN и определить сопоставление с второстепенной VLAN.

Для порта Trunk основной VLAN используйте команду **switchport mode trunk**, чтобы указать режим порта, и команду **switchport trunk allowed vlan**, чтобы определить связанные VLAN.

Для порта Trunk Promiscuous используйте команду **switchport mode private-vlan trunk promiscuous**, чтобы указать режим порта, и команду **switchport private-vlan mapping trunk**, чтобы определить связанные VLAN.

Для второстепенного порта Trunk используйте команду **switchport mode private-vlan trunk secondary**, чтобы указать режим порта, и команду **switchport private-vlan host-association trunk**, чтобы определить связанные VLAN.

При смене режима интерфейса настройки, связанные с предыдущим режимом, будут утеряны.

**Пример**

В данном примере показано, как настроить физические порты в качестве портов Private VLAN. Здесь Ethernet 1/0/1 указан как Host Port для Private VLAN, а Ethernet 1/0/2 указан как Promiscuous Port для Private VLAN.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# exit
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)#
```

## *24.5. switchport private-vlan host-association*

Данная команда используется для связи Private VLAN с портом Isolated, портом Community или второстепенным портом Trunk. При использовании формы **no** команда отменит связь.

**switchport private-vlan host-association [trunk]** *PRIMARY-VLAN-ID SECONDARY-VLAN-ID*

**no switchport private-vlan host-association [trunk** *PRIMARY-VLAN-ID SECONDARY-VLAN-ID***]**

**Параметры**

| | |
|---|---|
| **trunk** | (Опционально) Укажите, чтобы второстепенный порт Trunk был связан с членом Private VLAN. |
| *PRIMARY-VLAN-ID* | Укажите ID основной VLAN, которую необходимо ассоциировать. Диапазон доступных ID от 2 до 4094. |
| *SECONDARY-VLAN-ID* | Укажите ID второстепенной VLAN, которую необходимо ассоциировать. Диапазон доступных ID от 2 до 4094. |

**По умолчанию**

Нет.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Порт является Isolated портом, если второстепенная VLAN, указанная в команде, будет являться Isolated VLAN. Порт является Community портом, если второстепенная VLAN, указанная командой, является Community VLAN.

Без применения параметра **trunk** команда настроит порт в качестве нетегированного члена и указанной второстепенной VLAN, и основной VLAN.

Если команда используется второстепенным портом Trunk, порт настраивается в качестве тегированного члена указанной второстепенной и основной сети VLAN.

**Пример**

В данном примере показано, как связать Ethernet 1/0/1 с основной VLAN 1000 и второстепенной VLAN 1001.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 1000 1001
Switch(config-if)#
```

В данном примере показано, как задать Ethernet 1/0/2 режим Trunk Secondary Mode и связать его с основной VLAN 2000 и второстепенной VLAN 2001.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# switchport mode private-vlan trunk secondary
Switch(config-if)# switchport private-vlan host-association trunk 2000 2001
Switch(config-if)#
```

## *24.6. switchport private-vlan mapping*

Данная команда позволяет ассоциировать членство Private VLAN с портом Promiscuous или Trunk Promiscuous. При использовании формы **no** команда отменит ассоциирование.

**switchport private-vlan mapping [trunk]** *PRIMARY-VLAN-ID* **{add** *SECONDARY-VLAN-ID* **[, | -] | remove** *SECONDARY-VLAN-ID* **[, | -]}**

**no switchport private-vlan mapping [trunk** *PRIMARY-VLAN-ID***]**

**Параметры**

| | |
|---|---|
| **trunk** | (Опционально) Укажите, чтобы порт Trunk Promiscuous был связан с членством Private VLAN. |
| *PRIMARY-VLAN-ID* | Укажите основную VLAN для сопоставления. Диапазон доступных ID Primary VLAN от 2 до 4094. |
| **add** *SECONDARY-VLAN-ID* | Укажите, чтобы добавить членство в указанной второстепенной VLAN. Диапазон доступных ID Secondary VLAN от 2 до 4094. |
| **remove** *SECONDARY-VLAN-ID* | Укажите, чтобы удалить членство в указанной второстепенной VLAN. |
| **,** | (Опционально) Используется для перечисления нескольких VLAN или отделения одного диапазона номеров VLAN от предыдущего. Пробелы до и после запятой недопустимы. |

| | |
|---|---|
| **-** | (Опционально) Используется для обозначения диапазона номеров VLAN. Пробелы до и после дефиса недопустимы. |

**По умолчанию**

Нет.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Команда доступна для физического порта и настройки интерфейса port-channel.

Без применения параметра trunk команда настроит порт в качестве нетегированного члена указанной основной VLAN, и маркировки второстепенной VLAN.

**Пример**

В данном примере показано, как настроить Ethernet 1/0/2 в качестве порта Promiscuous для Private VLAN и сопоставить его с основной VLAN 1000 и второстепенными VLAN 1001 и VLAN 1002.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 1000 add 1001,1002
Switch(config-if)#
```

В данном примере показано, как настроить Ethernet 1/0/3 в качестве порта Trunk Promiscuous для Private VLAN и сопоставить его с основной VLAN 2000 и второстепенными VLAN 2001 и VLAN 2002.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# switchport mode private-vlan trunk promiscuous
Switch(config-if)# switchport private-vlan mapping trunk 2000 add 2001,2002
Switch(config-if)#
```

## *24.7. switchport private-vlan trunk native vlan*

Данная команда позволяет указать Native VLAN ID на порту Trunk Promiscuous для Private VLAN или второстепенном порту Trunk. При использовании формы **no** команда вернет настройки по умолчанию.

**switchport private-vlan trunk native vlan {***VLAN-ID* **| tag}**

**no switchport private-vlan trunk native vlan [tag]**

**Параметры**

| | |
|---|---|
| *VLAN-ID* | Укажите VLAN ID. Доступен диапазон значений от 2 до 4094. |
| **tag** | Укажите для включения режима Tagging Mode для Trunk Native VLAN. |

**По умолчанию**

По умолчанию Native VLAN 1, в режиме Untagged Mode.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Команда доступна для физического порта и настройки интерфейса port-channel.

Команда действует, только если интерфейсу задан режим Private VLAN Trunk Promiscuous или Trunk Secondary Mode.

Когда Trunk Native VLAN задана в режиме Tagged Mode, тип принимаемых кадров Acceptable frame type порта должен быть настроен только на прием тегированных кадров (**tagged-only**).

Когда порт Trunk Private VLAN работает в режиме Untagged mode для Native VLAN, передавая нетегированные пакеты для Native VLAN и тегированные пакеты для всех других VLAN, тип принимаемых кадров Acceptable frame type порта должен быть настроен как **admit-all**, чтобы функция работала корректно.

**Пример**

В данном примере показано, как настроить Ethernet 1/0/2 в качестве порта Native VLAN.

```
Switch# configure terminal
Switch(config)# interface eth5/0/2
Switch(config-if)# switchport private-vlan trunk native vlan 2
Switch(config-if)#
```

## *24.8. switchport private-vlan trunk allowed vlan*

Данная команда используется для поддержки Normal VLAN на порту Trunk Promiscuous или второстепенном порту Trunk. При использовании формы **no** команда вернет настройки по умолчанию.

**switchport private-vlan trunk allowed vlan {all | [add | remove | except]** *VLAN-ID* **[, | -]}**

**no switchport private-vlan trunk allowed vlan**

**Параметры**

| | |
|---|---|
| **all** | Укажите, чтобы добавить порт во все существующие VLAN. |
| **add** | Укажите, чтобы добавить порт в VLAN. |
| **remove** | Укажите, чтобы удалить порт из VLAN. |
| **except** | Указывает на добавление порта в VLAN. |
| *VLAN-ID* | Укажите VLAN ID. Доступен диапазон значений от 2 до 4094. |
| **,** | (Опционально) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы. |
| **-** | (Опционально) Укажите диапазон VLAN. Пробелы до и после дефиса недопустимы. |

**По умолчанию**

По умолчанию VLAN 1 разрешена.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Команда доступна для физического порта и настройки интерфейса port-channel.

Команда действует, только если интерфейсу задан режим Private VLAN Trunk Promiscuous mode или Trunk Secondary Mode.

Если VLAN разрешена на порту Trunk Private VLAN, порт станет тегированным членом VLAN.

Команда используется для поддержки Normal VLAN на портах Trunk Promiscuous или второстепенных портах Trunk. Пакет, принятый на порту Trunk Promiscuous может принадлежать основной VLAN или Normal VLAN в зависимости от входящей VLAN. Пакет, принятый на второстепенный порт Trunk может принадлежать второстепенной VLAN или Normal VLAN в зависимости от входящей VLAN.

**Пример**

В данном примере показано, как настроить второстепенный Trunk Ethernet 1/0/2 в качестве члена порта Normal VLAN 2.

```
Switch# configure terminal
Switch(config)# interface eth5/0/2
Switch(config-if)# switchport private-vlan trunk allowed vlan add 2
Switch(config-if)#
```

## *24.9. show vlan private-vlan*

Данная команда используется для просмотра настроек Private VLAN.

**show vlan private-vlan**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Команда используется для отображения списка Private VLAN, находящегося в домене VLAN, ассоциации второстепенного VLAN с основным VLAN и портов каждого Private VLAN.

**Пример**

В данном примере показано, как включить отображение настроек Private VLAN. В данном примере настроено 2 домена Private VLAN.

```
Switch# show vlan private-vlan

Primary VLAN   Secondary VLAN   Type           Interface
-------------  --------------  ----------  ----------------------------
1000            1001              isolated      eth1/0/1, eth1/0/16
                1002              community
                1003              community
2000            2001              isolated      eth1/0/2, eth1/0/3
2000            2002              community     eth1/0/2, eth1/0/3
2000            2003              community     eth1/0/4, eth1/0/13, eth1/0/15

Total Entries: 6

Switch#
```

# 25. Команды System Log

## *25.1. clear logging*

Данная команда используется для удаления сообщений из внутреннего буфера.

**clear logging**

**Параметры**

Нет.

**По умолчанию**

Нет.

**Режим ввода команды**

Privileged EXEC Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Команда удаляет все сообщения из внутреннего буфера.

**Пример**

В примере показано, как удалить все сообщения из внутреннего буфера.

```
Switch# clear logging

Clear logging? (y/n) [n] y

Switch#
```

## *25.2. logging on*

Данная команда используется для включения логирования системных сообщений. При использовании формы **no** команда отключит логирование системных сообщений.

**logging on**
**no logging on**

**Параметры**

Нет.

**По умолчанию**

По умолчанию опция включена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Для включения логирования системных сообщений используйте команду **logging on** в режиме Global Configuration Mode. Данная команда регистрирует отладочные сообщения (debug) и сообщения об ошибках (error) в системном журнале (логе). Процесс сохранения сообщений идет асинхронно процессам, генерирующим данные сообщения. Используйте форму **no** для

отключения данной функции.

Процесс логирования контролирует распределение сообщений по нескольким направлениям, таким как буфер логирования, консоль или syslog-сервер. Для включения или отключения функции логирования для каждого направления индивидуально можно использовать команды глобального режима конфигурирования **logging buffered** и **logging server.** Однако если команда **logging on** отключена, сообщения по данным направлениям отправляться не будут. Если команда **logging on** включена, одновременно с ней будет активирована команда **logging buffered**.

**Пример**

В данном примере показано, как включить логирование системных сообщений.

```
Switch# configure terminal
Switch(config)# logging on
WARNING: The command takes effect and the logging buffered is enabled at the same time
Switch(config)#
```

## *25.3. logging buffered*

Данная команда используется для включения логирования системных сообщений во внутренний буфер. При использовании формы **no** команда отключит логирование системных сообщений во внутренний буфер. Используйте команду **default logging buffered**, чтобы вернуть настройки по умолчанию.

**logging buffered [severity {***SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [discriminator** *NAME***] [write-delay {***SECONDS* **|** infinite**}]**

**no logging buffered**

**default logging buffered**

**Параметры**

| | |
|---|---|
| *SEVERITY-LEVEL* | (Опционально) Укажите уровень важности системных сообщений. Сообщения с заданным уровнем важности или выше передаются во внутренний буфер. Доступны значения от 0 до 7, где 0 – наиболее высокий уровень важности. Уровни важности сообщений:<br>**0** – emergencies – чрезвычайные ситуации, система не работоспособна,<br>**1** – alerts – тревога, система требует немедленного вмешательства,<br>**2** – critical – состояние системы критическое,<br>**3** – errors – сообщения об ошибках,<br>**4** – warnings – предупреждения о возможных проблемах,<br>**5** – notifications – уведомления о нормальных, но важных событиях,<br>**6** – informational – информационные сообщения,<br>**7** – debugging – отладочные сообщения.<br>Если значение не указано, по умолчанию используется уровень важности warnings (**4**). |
| *SEVERITY-NAME* | (Опционально) Укажите название уровня важности системных сообщений: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7). |
| **discriminator** | (Опционально) Укажите discriminator для фильтрации сообщений, отправляемых во внутренний буфер. |
| **write-delay** *SECONDS* | (Опционально) Укажите, чтобы отложить периодическую запись буфера логирования во FLASH на указанное количество секунд. |

**По умолчанию**

По умолчанию используется уровень важности warning (4).

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Системные сообщения можно передать в локальный буфер и другие точки назначения. Перед отправкой в другие точки назначения сообщения должны поступить в локальный буфер.

Команда не применяется, если указанный discriminator не существует. В этом случае применяются настройки по умолчанию.

Укажите уровень важности сообщений для ограничения системных сообщений, логируемых в буфер (это позволит уменьшить количество зарегистрированных сообщений). Сообщения указанного уровня или выше логируются в буфер. При заполнении буфера старые записи удаляются, чтобы освободить место для новых сообщений.

Содержимое буфера периодически сохраняется во FLASH-память, чтобы при перезагрузке сообщения можно было восстановить. При необходимости можно задать интервал для сохранения записей из буфера во FLASH-память. При перезагрузке содержимое сообщений, сохраняемых во FLASH, будет перезагружено в буфер логирования.

**Пример**

В данном примере показано, как включить логирование сообщений в буфер и ограничить логирование сообщений с уровнем важности errors или выше.

```
Switch# configure terminal
Switch(config)# logging buffered severity errors
Switch(config)#
```

## *25.4. logging console*

Данная команда используется для включения логирования системных сообщений в локальной консоли. При использовании формы **no** команда отключит логирование сообщений в локальной консоли и вернет настройки по умолчанию.

**logging console [severity {***SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [discriminator** *NAME***]**

**no logging console**

**Параметры**

| | |
|---|---|
| *SEVERITY-LEVEL* | (Опционально) Укажите уровень важности системных сообщений. Сообщения с заданным уровнем важности или выше передаются во внутренний буфер. Доступны значения от 0 до 7, где 0 – наиболее высокий уровень важности.<br>Уровни важности сообщений:<br>**0** – emergencies – чрезвычайная ситуация, система не работоспособна,<br>**1** – alerts – тревога, система требует немедленного вмешательства,<br>**2** – critical – состояние системы критическое,<br>**3** – errors – сообщения об ошибках,<br>**4** – warnings – предупреждения о возможных проблемах,<br>**5** – notifications – уведомления о нормальных, но важных событиях, |

| | |
|---|---|
| | **6** – informational – информационные сообщения,<br>**7** – debugging – отладочные сообщения.<br>Если значение не указано, по умолчанию используется уровень важности warnings (**4**). |
| *SEVERITY-NAME* | (Опционально) Укажите название уровня важности системных сообщений: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7). |
| **discriminator** | (Опционально) Укажите discriminator для фильтрации сообщений, отправляемых в локальный буфер. |

**По умолчанию**

По умолчанию опция отключена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Системные сообщения можно логировать в локальный буфер сообщений, локальную консоль или другие точки назначения. Перед отправкой на консоль сообщения должны предварительно поступить в локальный буфер.

Команда не применяется, если указанный discriminator не существует. В этом случае будут применяться настройки по умолчанию.

Укажите уровень важности сообщений для ограничения системных сообщений, логируемых в консоли. Сообщения указанного уровня или выше будут логироваться в локальную консоль.

**Пример**

В данном примере показано, как включить логирование сообщений в локальную консоль и ограничить логирование сообщений с уровнем важности errors или выше.

```
Switch# configure terminal
Switch(config)# logging console severity errors
Switch(config)#
```

## *25.5. logging discriminator*

Данная команда используется при создании discriminator для дальнейшей фильтрации сообщений SYSLOG, отправляемых в различные точки назначения. При использовании формы **no** команда удалит discriminator.

**logging discriminator** *NAME* **[facility {drops** *STRING* **| includes** *STRING***}] [severity {drops** *SEVERITY-LIST* **| includes** *SEVERITY-LIST***}]**

**no discriminator** *NAME*

**Параметры**

| | |
|---|---|
| *NAME* | Укажите имя discriminator. |
| **facility** | (Опционально) Укажите, чтобы использовать подфильтр на основе категории facility. |
| *STRING* | Укажите одно или более имен facility. Если используется несколько |

| | |
|---|---|
| | имен, они должны быть разделены запятой без пробелов. |
| **includes** | Укажите для включения совпадающих сообщений. Несовпадающие сообщения будут фильтроваться. |
| **drops** | Укажите для фильтрации совпадающих сообщений. |
| **severity** | (Опционально) Укажите подфильтр на основе совпадений с уровнем важности. |
| *SEVERITY- LIST* | Укажите список уровней важности для фильтрации или включения. |

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Настраивается существующий параметр discriminator. При вводе команды предыдущие настройки будут заменены новыми. Ассоциируйте discriminator с командами **logging buffered** и **logging server**.

**Пример**

В данном примере показано, как создать discriminator с именем «buffer-filter», указывающим два подфильтра: один на основе уровня важности, а другой на основе facility.

```
Switch# configure terminal
Switch(config)# logging discriminator buffer-filter facility includes STP severity includes 1-4,6
Switch(config)#
```

## *25.6. logging server*

Данная команда используется для включения логирования системных сообщений на указанный SYSLOG-сервер. При использовании формы **no** команда удалит SYSLOG-сервер с указанным адресом из списка SYSLOG-серверов.

**logging server {***IP-ADDRESS* **|** *IPV6-ADDRESS***} [vrf** *VRF-NAME***] [severity {***SEVERITY-LEVEL* **|** *SEVERITY-NAME***}]** [facility **{***FACILITY-NUM* **|** *FACILITY-NAME***}] [discriminator** *NAME***] [port** *UDP-PORT***]**

**no logging server {***IP-ADDRESS* **|** *IPV6-ADDRESS***} [vrf** *VRF-NAME***]**

**Параметры**

| | |
|---|---|
| *IP-ADDRESS* | Укажите IP-адрес SYSLOG-сервера. |
| *IPV6-ADDRESS* | Укажите IPv6-адрес серверного узла логирования. |
| *VRF-NAME* | Укажите имя VRF Instance. |

| | |
|---|---|
| *SEVERITY-LEVEL* | (Опционально) Укажите уровень важности системных сообщений. Сообщения с заданным уровнем важности или выше передаются во внутренний буфер. Доступны значения от 0 до 7, где 0 – наиболее высокий уровень важности.<br>Уровни важности сообщений:<br>**0** – emergencies – чрезвычайная ситуация, система не работоспособна,<br>**1** – alerts – тревога, система требует немедленного вмешательства,<br>**2** – critical – состояние системы критическое,<br>**3** – errors – сообщения об ошибках,<br>**4** – warnings – предупреждения о возможных проблемах,<br>**5** – notifications – уведомления о нормальных, но важных событиях,<br>**6** – informational – информационные сообщения,<br>**7** – debugging – отладочные сообщения.<br>Если значение не указано, по умолчанию используется уровень важности warnings (**4**). |
| *SEVERITY-NAME* | (Опционально) Укажите название уровня важности системных сообщений: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7). |
| *FACILITY-NUM* | (Опционально) Укажите десятичное значение от 0 до 23 для категории facility. Если значение не указано, по умолчанию будет использоваться **local7** (23). Для более подробной информации обратитесь к параграфу Использование команды. |
| *FACILITY-NAME* | (Опционально) Укажите имя facility. Если значение не указано, по умолчанию будет использоваться local7 (23). Для более подробной информации обратитесь к параграфу Использование команды. |
| **discriminator** | (Опционально) Укажите для фильтрации сообщений на сервер логирования согласно настройке discriminator. |
| **port** *UDP-PORT* | (Опционально) Укажите номер порта UDP, который будет использоваться сервером SYSLOG. Доступен диапазон значений от 1024 до 65535, а также 514 (распространенный порт IANA). Если значение не указано, номер UDP-порта по умолчанию – 514. |

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Системные сообщения можно логировать в локальный буфер сообщений, на локальную консоль или удаленные узлы. Перед отправкой на сервер логирования сообщения должны поступить в локальный буфер сообщений.

Таблица 25.1. Значения Facility

| Номер Facility | Имя Facility | Описание |
|---|---|---|
| 0 | kern | Сообщения ядра |
| 1 | user | Сообщения пользовательского уровня |
| 2 | mail | Почтовая система |
| 3 | daemon | Системные службы (daemons) |
| 4 | auth1 | Сообщения системы безопасности/авторизации |
| 5 | syslog | Сообщения, генерируемые SYSLOG |
| 6 | lpr | Подсистема печати (Line Printer) |
| 7 | news | Подсистема сетевых новостей |
| 8 | uucp | Подсистема UUCP |
| 9 | clock1 | Службы времени (Clock daemon) |
| 10 | auth2 | Сообщения системы безопасности/авторизации |
| 11 | ftp | Служба FTP |
| 12 | ntp | Подсистема NTP |
| 13 | logaudit | Журнал аудита |
| 14 | logalert | Аварийный журнал |
| 15 | clock2 | Служба времени (примечание 2) |
| 16 | local0 | Локальное использование 0 (local0) |
| 17 | local1 | Локальное использование 1 (local1) |
| 18 | local2 | Локальное использование 2 (local2) |
| 19 | local3 | Локальное использование 3 (local3) |
| 20 | local4 | Локальное использование 4 (local4) |
| 21 | local5 | Локальное использование 5 (local5) |
| 22 | local6 | Локальное использование 6 (local6) |
| 23 | local7 | Локальное использование 7 (local7) |

**Пример**

В данном примере показано, как включить логирование системных сообщений с уровнем важности выше warnings на удаленном узле 20.3.3.3.

```
Switch# configure terminal
Switch(config)# logging server  20.3.3.3 severity warnings
Switch(config)#
```

## *25.7. logging smtp*

Данная команда позволяет настроить отправку логов на электронную почту. При использовании формы **no** команда отключит отправку системных сообщений на электронную почту и вернет настройки по умолчанию.

**logging smtp [severity {***SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [discriminator** *NAME***]**

**no logging smtp**

**Параметры**

| | |
|---|---|
| *SEVERITY-LEVEL* | (Опционально) Укажите уровень важности системных сообщений. Сообщения с заданным уровнем важности или выше передаются во внутренний буфер. Доступны значения от 0 до 7, где 0 – наиболее высокий уровень важности. Уровни важности сообщений:<br>**0** – emergencies – чрезвычайная ситуация, система не работоспособна,<br>**1** – alerts – тревога, система требует немедленного вмешательства,<br>**2** – critical – состояние системы критическое,<br>**3** – errors – сообщения об ошибках,<br>**4** – warnings – предупреждения о возможных проблемах,<br>**5** – notifications – уведомления о нормальных, но важных событиях,<br>**6** – informational – информационные сообщения,<br>**7** – debugging – отладочные сообщения.<br>Если значение не указано, по умолчанию используется уровень важности warnings (**4**). |
| *SEVERITY-NAME* | (Опционально) Укажите название уровня важности системных сообщений. Имена уровней важности: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7). |
| **discriminator** | (Опционально) Укажите для фильтрации сообщений, отправляемых на почту, на основе значения discriminator. |

**По умолчанию**

По умолчанию опция отключена.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Системные сообщения можно логировать на электронную почту. Данная команда не применяется, если указанный discriminator не существует. В этом случае будут применяться настройки по умолчанию. Сообщения необходимо логировать в локальный буфер перед отправкой на электронную почту.

Укажите уровень важности сообщений для ограничения системных логируемых сообщений. Сообщения указанного уровня или выше будут логироваться на электронную почту.

**Пример**

В данном примере показано, как включить логирование системных сообщений с уровнем важности выше warnings на электронную почту.

```
Switch# configure terminal
Switch(config)# logging smtp severity warnings
Switch(config)#
```

## 25.8. logging source-interface

Данная команда позволяет задать IP-адрес интерфейса, который будет использоваться в качестве адреса источника для отправки пакетов SYSLOG. При использовании формы **no** команда вернет настройки по умолчанию.

**logging source-interface** *INTERFACE-ID*

**no logging source-interface**

**Параметры**

| | |
|---|---|
| *INTERFACE-ID* | Укажите IP-адрес интерфейса, который будет использоваться в качестве адреса источника для отправки пакетов SYSLOG. |

**По умолчанию**

По умолчанию используется IP-адрес ближайшего интерфейса.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте данную команду, чтобы задать IP-адрес 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 vlan100
Switch(config)#
```

## 25.9. show logging

Данная команда используется для просмотра системных сообщений, хранящихся во внутреннем буфере.

**show logging [all | [***REF-SEQ***] [+** *NN* **|** - *NN***]]**

**Параметры**

| | |
|---|---|
| **all** | Укажите для вывода всех записей журнала, начиная с последних. |
| *REF-SEQ* | Укажите порядковый номер, с которого начнется вывод записей. |

| | |
|---|---|
| **+** *NN* | Укажите количество сообщений, которое необходимо отобразить после указанного порядкового номера. Если номер не указан, отображение начинается с самого раннего сообщения в буфере. |
| **-** *NN* | Укажите количество сообщений, которое необходимо отобразить до указанного номера. Если номер не указан, отображение начинается с последнего сообщения в буфере. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Команда используется для просмотра сообщений, хранящихся во внутреннем буфере.

Каждое сохраненное в буфер сообщение соотносится с определенным порядковым номером. При регистрации сообщению назначается порядковый номер, начиная с 1. При достижении значения 100000 нумерация вновь начнется с 1.

Если задается количество сообщений, которые необходимо отобразить после указанного порядкового номера, то вывод сообщений начнется с более ранних записей. Если задается количество сообщений, которые предшествуют указанному порядковому номеру, то вывод сообщений начнется с более поздних записей.

Если команда введена без опций, система выводит 200 записей, начиная с последнего сообщения.

**Пример**

В данном примере показано, как отобразить сообщения в локальном буфере сообщений.

```
Switch# show Switch# show logging

Total number of buffered messages: 2
#2 2015-03-25 16:37:36 Unit 1, Successful login through Console (Username: Anonymous)
#1 2015-03-25 16:35:54 INFO(6) Port eth1/0/1 link up, 1000Mbps FULL duplex

Switch#
```

## *25.10. show attack-logging*

Данная команда используется для просмотра зарегистрированных сообщений об атаках.

**show attack-logging unit** *UNIT-ID* **[index** *INDEX***]**

**Параметры**

| | |
|---|---|
| *UNIT-ID* | Укажите модуль (Unit), для которого необходимо отобразить зарегистрированные сообщения об атаке. |
| *INDEX* | Укажите список порядковых номеров записей, которые необходимо отобразить. Если значение не указано, отображаться будут все записи из журнала атак. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для просмотра сообщений об атаках в журнале. К таким сообщениям относятся записи, связанные с функционалом DOS и port-security. В этом случае может генерироваться большое количество подобных сообщений, из-за чего в системе быстро заканчивается память для хранения записей журнала. Чтобы этого избежать, в системный журнал сохраняется только первое сообщение данного типа, генерируемое каждую минуту, а остальные хранятся в отдельной таблице с именем attack log (журнал атак).

**Пример**

В данном примере показано, как отобразить первое зарегистрированное сообщение об атаке.

```
Switch# show attack-logging index 1
Attack log messages:
1  2015-03-24 15:00:14 CRIT(2) Land attack is blocked from (IP: 10.72.24.1 Port: 7)
Switch#
```

## *25.11. clear attack-logging*

Данная команда используется для удаления сообщений об атаках.

**clear attack-logging {unit** *UNIT-ID* **| all}**

**Параметры**

| | |
|---|---|
| **unit** *UNIT-ID* | Укажите модуль (Unit), для которого необходимо удалить зарегистрированные сообщения об атаке. |
| **all** | Укажите для удаления всех записей. |

**По умолчанию**

Нет.

**Режим ввода команды**

Privileged EXEC Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда используется для удаления сообщений об атаках.

**Пример**

В данном примере показано, как удалить все логированные сообщения об атаках.

```
Switch# clear attack-logging all
Switch#
```

# 26. Команды VLAN (Virtual LAN)

## *26.1. acceptable-frame*

Данная команда используется для настройки допустимых типов кадров, которые будут приниматься на порту. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**acceptable-frame {tagged-only | untagged-only | admit-all}**

**no acceptable-frame**

**Параметры**

| | |
|---|---|
| **tagged-only** | Допускаются только тегированные кадры. |
| **untagged-only** | Допускаются только нетегированные кадры. |
| **admit-all** | Допускаются все кадры. |

**По умолчанию**

Для режима Access VLAN опцией по умолчанию является **untagged-only**.

Для других режимов VLAN 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 порт Ethernet 1/0/1, чтобы он принимал только тегированные кадры **tagged-only**.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# acceptable-frame tagged-only
Switch(config-if)#
```

## *26.2. ingress-checking*

Данная команда используется для включения проверки входящих кадров, получаемых портом. Используйте форму **no** для отключения проверки.

**ingress-checking**

**no ingress-checking**

**Параметры**

Нет.

**По умолчанию**

По умолчанию данная опция включена.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте данную команду для включения проверки входящих кадров, получаемых интерфейсом. Если проверка включена, и принимающий порт не является членом VLAN, классифицированной для получения пакета, то пакет отбрасывается.

**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)#
```

## *26.3. mac-vlan*

Данная команда используется для создания VLAN на основе MAC-адреса. Используйте форму **no** для удаления VLAN на основе MAC-адреса.

**mac-vlan** *MAC-ADDRESS* **vlan** *VLAN-ID* **[priority** *COS-VALUE***]**

**no mac-vlan** *MAC-ADDRESS*

**Параметры**

| | |
|---|---|
| *MAC-ADDRESS* | MAC-адрес для привязки. |
| **vlan** *VLAN-ID* | VLAN ID для создания VLAN на основе MAC-адреса. |
| **priority** *COS-VALUE* | (Опционально) Значение приоритета CoS. Если параметр не указан, то значением CoS по умолчанию является 0. |

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте данную команду для создания VLAN на основе MAC-адреса. Классификация будет применена к пакетам, получаемым коммутатором. По умолчанию приоритет для классификации VLAN для нетегированного пакета является MAC-based > Subnet-based > Protocol VLAN.

**Пример**

В данном примере показано, как создать привязку VLAN ID на основе MAC-адреса для MAC-адреса 00-80-cc-00-00-11.

```
Switch# configure terminal
Switch(config)# mac-vlan 00-80-cc-00-00-11 vlan 101 priority 4
Switch(config)#
```

## *26.4. protocol-vlan profile*

Данная команда используется для создания группы протоколов. Используйте форму **no** для удаления указанной группы протоколов.

**protocol-vlan profile** *PROFILE-ID* **frame-type {ethernet2 | snap | llc} ether-type** *TYPE-VALUE*

**no protocol-vlan profile** *PROFILE-ID*

**Параметры**

| | |
|---|---|
| *PROFILE-ID* | Группа протоколов, которую необходимо добавить или удалить. |
| **frame-type** | Тип кадров. |
| **ethernet2** | Значение для типа кадров Ethernet II. |
| **snap** | Значение для типа кадров SNAP. |
| **llc** | Значение для типа кадров LLC. |
| **ether-type** *TYPE-VALUE* | Указывается тип пакетов. Данное значение должно быть 2-байтным в шестнадцатиричной форме. |

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте команду **protocol-vlan profile** в режиме Global Configuration Mode для создания группы протоколов. Затем используйте команду **protocol-vlan profile** в режиме Interface Configuration Mode для настройки классификации VLAN для группы протоколов, получаемых на порту.

**Пример**

В данном примере показано, как создать VLAN-группу протоколов с идентификатором группы 10, указав, что будет использоваться протокол IPv6 (тип кадров – Ethernet2, значение – 0x86dd).

```
Switch# configure terminal
Switch(config)# protocol-vlan profile 10 frame-type ethernet2 ether-type 0x86dd
Switch(config)#
```

## *26.5. protocol-vlan profile (interface)*

Данная команда используется для настройки привязки VLAN для группы протоколов на порту. Используйте форму **no** для удаления привязки VLAN на порту.

**protocol-vlan profile** *PROFILE-ID* **vlan** *VLAN-ID* **[priority** *COS-VALUE***]**

**no protocol-vlan profile** *PROFILE-ID*

**Параметры**

| | |
|---|---|
| *PROFILE-ID* | Идентификатор группы протоколов, который должен классифицироваться. |

| | |
|---|---|
| *VLAN-ID* | VLAN ID для protocol VLAN. Для каждой группы привязки может быть указан только один VLAN ID. |
| **priority** *COS-VALUE* | (Опционально) Значение приоритета CoS. Если параметр не указан, то значением CoS по умолчанию является 0. |

**По умолчанию**

Нет.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте данную команду, чтобы указать VLAN для группы протоколов на порту. В результате пакет, полученный на порту, который соответствует указанной группе протоколов, будет определен в указанную VLAN. VLAN не должна обязательно существовать для настройки команды. Приоритет классификации VLAN для нетегированного пакета является MAC-based > Subnet-based > Protocol VLAN.

**Пример**

В данном примере показано, как создать привязку VLAN на Ethernet 1/0/1 для классификации пакетов в группе протоколов 10 в VLAN 3000.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# protocol-vlan profile 10 vlan 3000
Switch(config-if)#
```

## *26.6. subnet-vlan*

Команда **subnet-vlan ipv4** используется для настройки привязки VLAN для подсети IPv4. Команда **subnet-vlan ipv6** используется для настройки привязки VLAN для подсети IPv6. Используйте форму **no** для удаления привязки VLAN на основе подсети.

**subnet-vlan {ipv4** *NETWORK-PREFIX NETWORK-MASK* **| ipv6** *IPV6-NETWORK PREFIX/PREFIX-LENGTH***} vlan** *VLAN-ID* **[priority** *COS-VALUE***]**

**no subnet-vlan {ipv4** *NETWORK-PREFIX NETWORK-MASK* **| ipv6** *IPV6-NETWORK-PREFIX/PREFIX-LENGTH***}**

**Параметры**

| | |
|---|---|
| **ipv4** *NETWORK-PREFIX*<br>*NETWORK-MASK* | Адрес сети IPv4 и маска подсети. |
| **ipv6** *IPV6-NETWORK-PREFIX/PREFIX-LENGTH* | IPv6-префикс и его длина. Длина IPv6-префикса не может превышать 64 бита. |
| **priority** *COS-VALUE* | (Опционально) Значение приоритета CoS. Если параметр не указан, то значением CoS по умолчанию является 0. |

**По умолчанию**

Нет.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте команду **subnet-vlan ipv4** для настройки привязки VLAN для подсети IPv4.

Используйте команду **subnet-vlan ipv6** для настройки привязки VLAN для подсети IPv6.

Классификация применяется к пакетам, полученным коммутатором. По умолчанию классификация VLAN для нетегированного пакета выполняется в следующей последовательности: MAC-based > Subnet-based > Protocol VLAN.

**Пример**

В данном примере показано, как настроить привязки VLAN для определения того, что пакеты принадлежат подсетям 20.0.0.0/8, 192.0.0.0/8 и 3ffe:22:33:44::/64 в VLAN 100.

```
Switch# configure terminal
Switch(config)# subnet-vlan ipv4 20.0.0.0/8 vlan 100 vlan 100
Switch(config)# subnet-vlan ipv4 192.0.0.0/8 vlan 100 priority 4
Switch(config)# subnet-vlan ipv6 3ffe:22:33:44::/64 vlan 100
Switch(config)#
```

## *26.7. show protocol-vlan profile*

Данная команда используется для отображения параметров настройки, касающихся protocol VLAN.

**show protocol-vlan {profile [***PROFILE-ID* **[, | -]] | interface** *[INTERFACE-ID* **[, | -]]}**

**Параметры**

| | |
|---|---|
| *PROFILE-ID* | (Опционально) Группа протоколов, которая должна отображаться. |
| **interface** *INTERFACE-ID* | (Опционально) Порт для отображения настроек классификации protocol VLAN. |
| **,** | (Опционально) Диапазон интерфейсов или отделение интерфейсов от предыдущего диапазона. Перед и после запятой использование пробела недопустимо. |
| **-** | (Опционально) Диапазон интерфейсов. Перед и после дефиса использование пробела недопустимо. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Используйте данную команду для отображения настроек для классификации VLAN на порту на основе группы протоколов.

**Пример**

В данном примере показано, как отобразить настройки для классификации VLAN на основе группы протоколов на портах Ethernet с 1/0/1 по 1/0/3.

```
Switch# show protocol-vlan interface ethernet 1/0/1-3

Interface    Protocol Group ID     VLAN    Priority
------------ --------------------- ------- ---------
eth1/0/1     1                     1       5
eth1/0/2     10                    3       0
             11                    2001    4
             12                    3002    1
eth1/0/3     2                     100     6

Switch#
```

В данном примере показано, как отобразить настройки профиля группы протоколов.

```
Switch# show protocol-vlan profile

 Profile ID  Frame-type   Ether-type
 ----------  -----------  ----------------
 1           Ethernet2    0x86DD(IPv6)
 2           Ethernet2    0x0800(IP)
 3           Ethernet2    0x0806(ARP)

Total Entries: 3

Switch#
```

## *26.8. show vlan*

Данная команда используется для отображения параметров для всех настроенных VLAN или одной VLAN на коммутаторе.

**show vlan [***VLAN-ID* **[, | -] | interface [***INTERFACE-ID* **[, | -]] | mac-vlan | subnet-vlan]**

**Параметры**

| | |
|---|---|
| *VLAN-ID* | (Опционально) Список VLAN для отображения информации о портах-участниках. Если VLAN не указана, то отображаются все VLAN. Допустимый диапазон: от 1 до 4094. |
| **interface** *INTERFACE-ID* | (Опционально) Порт для отображения настроек VLAN. |
| **,** | (Опционально) Диапазон интерфейсов или отделение интерфейсов от предыдущего диапазона. Использование пробела до и после запятой недопустимо. |
| **-** | (Опционально) Диапазон интерфейсов. Использование пробела до и после дефиса недопустимо. |
| **mac-vlan** | (Опционально) Указывается для отображения информации о VLAN на основе MAC-адресов. |

| | |
|---|---|
| **subnet-vlan** | (Опционально) Указывается для отображения информации о VLAN на основе подсетей (subnet). |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Данная команда используется для отображения параметров одной или всех настроенных на коммутаторе VLAN.

**Пример**

В данном примере показано, как отобразить все текущие записи VLAN.

```
Switch# show vlan

VLAN 1
   Name : default
   Tagged Member Ports   :
   Untagged Member Ports : 1/0/1-1/0/8

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

eth1/0/1
VLAN mode              : Trunk
Native VLAN            : 5 (Untagged)
Trunk allowed VLAN     : 2,4,5,6
Ingress checking       : Enabled
Acceptable frame type  : Admit-all
Dynamic Tagged VLAN    : 100

eth1/0/2
VLAN mode              : Access
Access VLAN            : 2
Ingress checking       : Enabled
Acceptable frame type  : Untagged-only

eth1/0/3
```

```
VLAN mode               : Hybrid
Native VLAN             : 5
Hybrid untagged VLAN    : 2,4,5,6
Hybrid tagged VLAN      : 8,9,10
Ingress checking        : Enabled
Acceptable frame type   : Admit-All
Dynamic tagged VLAN     :
VLAN Precedence         : MAC-VLAN

eth1/0/4
VLAN mode               : Dot1q-tunnel
Access VLAN             : 800
Hybrid untagged VLAN    : 200, 600
Ingress checking        : Enabled
Acceptable frame type   : Admit-all
VLAN Precedence         : MAC-VLAN

Switch#
```

В данном примере показано, как отобразить все привязки VLAN на основе MAC-адресов.

```
Switch# show vlan mac-vlan

MAC Address         VLAN ID   Priority  Status
 ------------------  --------  --------  ----------
 00-80-cc-00-00-11   101         4       Active
 00-11-22-00-00-05   200         5       Active

Total Entries: 2

Switch#
```

В данном примере показано, как отобразить все привязки VLAN на основе подсетей.

```
Switch# show vlan subnet-vlan

 Subnet                    VLAN ID  Priority
 ------------------------  -------  ---------
 20.0.0.0/8                100      0
 192.0.0.0/8               100      4
 3FFE:22:33:44::/64        100      0

Total Entries: 3

Switch#
```

## *26.9. switchport access vlan*

Данная команда используется для указания access VLAN для интерфейса. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**switchport access vlan** *VLAN-ID*

**no switchport access vlan**

**Параметры**

| | |
|---|---|
| **access vlan** *VLAN-ID* | Access VLAN интерфейса. |

**По умолчанию**

По умолчанию access VLAN является VLAN 1.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда вступает в силу, когда интерфейс настроен в режиме доступа (access mode) или режиме dot1q-tunnel mode. VLAN, указанная в качестве access VLAN, не должна обязательно существовать для настройки команды.

Может быть указана только одна access VLAN. Следующая команда перезаписывает предыдущую.

**Пример**

В данном примере показано, как настроить интерфейс доступа ethernet 1/0/1 для 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)#
```

## *25.10. switchport hybrid allowed vlan*

Данная команда используется для указания тегированных или нетегированных VLAN для гибридного порта. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**switchport hybrid allowed vlan {[add] {tagged | untagged} | remove}** *VLAN-ID* **[, | -]**

**no switchport hybrid allowed vlan**

**Параметры**

| | |
|---|---|
| **add** | Порт, который будет добавлен в указанную(-ые) VLAN. |
| **remove** | 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 одного диапазона номеров VLAN от предыдущего. Использование пробела до и после запятой недопустимо. |
| **-** | (Опционально) Используется для диапазона номеров VLAN. Использование пробела до и после дефиса недопустимо. |

**По умолчанию**

По умолчанию гибридный порт является нетегированным членом VLAN 1.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

При многократном использовании команды hybrid VLAN 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 частично совпадает с текущим списком тегированных разрешенных VLAN, то совпадающая часть будет изменена на нетегированную разрешенную VLAN. С другой стороны, если новый список тегированных разрешенных VLAN частично совпадает с текущим списком нетегированных разрешенных VLAN, то совпадающая часть будет изменена на тегированную разрешенную VLAN. В силу вступает последняя заданная команда. Необязательно создавать VLAN, чтобы настроить данную команду.

**Пример**

В данном примере показано, как настроить 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)#
```

## *26.11. switchport hybrid native vlan*

Данная команда используется для указания native VLAN ID гибридного порта. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**switchport hybrid native vlan** *VLAN-ID*

**no switchport hybrid native vlan**

**Параметры**

| | |
|---|---|
| *VLAN-ID* | Native VLAN гибридного порта. |

**По умолчанию**

По умолчанию native VLAN гибридного порта является VLAN 1.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

При настройке привязки гибридного порта к его native VLAN используйте команду **switchport hybrid allowed vlan**, чтобы добавить native VLAN в список разрешенных VLAN. Указанная VLAN не должна обязательно существовать для применения этой команды. Команда вступает в силу, когда интерфейс настроен на работу в гибридном режиме.

**Пример**

В данном примере показано, как настроить ethernet 1/0/1 в качестве гибридного интерфейса и задать PVID со значением 20.

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

## *26.12. switchport mode*

Данная команда используется для настройки режима работы порта в VLAN. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**switchport mode {access | hybrid | trunk | dot1q-tunnel}**

**no switchport mode**

**Параметры**

| | |
|---|---|
| **access** | Указывает порт в качестве порта доступа. |
| **hybrid** | Указывает порт в качестве гибридного порта. |
| **trunk** | Указывает порт в качестве trunk-порта. |
| **dot1q-tunnel** | Указывает порт в качестве порта dot1q-tunnel. |

**По умолчанию**

По умолчанию установлена опция **hybrid**.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

В режиме **access** порт выступает в качестве нетегированного члена access VLAN, заданной для данного порта. В режиме **hybrid** порт может быть нетегированным или тегированным членом всех настроенных VLAN. Цель этого режима VLAN - поддержка protocol VLAN, VLAN на основе подсетей (subnet-based VLAN) и VLAN на основе MAC-адресов (MAC-based VLAN).

В режиме **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. В режиме **dot1q-tunnnel mode** порт действует как порт UNI в service VLAN.

При изменении режима работы порта настройки, связанные с VLAN и ассоциированные с предыдущим режимом, будут утеряны.

**Пример**

В примере ниже показано, как настроить ethernet 1/0/1 в качестве trunk-порта.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)#
```

## *26.13. switchport trunk allowed vlan*

Данная команда используется для настройки VLAN, которым разрешено получать и отправлять трафик на указанный интерфейс в тегированном формате. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**switchport trunk allowed vlan {all | [add | remove | except]** *VLAN-ID* **[, | -]}**

**no switchport trunk allowed vlan**

**Параметры**

| | |
|---|---|
| **all** | Указывает, что на интерфейсе разрешены все VLAN. |
| **add** | Добавление указанного списка VLAN в список разрешенных VLAN. |
| **remove** | Удаление указанного списка 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 одного диапазона VLAN от предыдущего. Использование пробела до и после запятой недопустимо. |
| **-** | (Опционально) Используется для диапазона номеров VLAN. Использование пробела до и после дефиса недопустимо. Использование пробела дефисом и после дефиса использование пробела недопустимо. |

**По умолчанию**

По умолчанию все VLAN разрешены.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Данная команда вступает в силу, только когда интерфейс работает в режиме trunk. 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 примере ниже показано, как настроить ethernet 1/0/1 в качестве тегированного члена VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 1000
Switch(config-if)#
```

## *26.14. switchport trunk native vlan*

Данная команда используется для указания native VLAN ID интерфейса в режиме trunk mode. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**switchport trunk native vlan {***VLAN-ID* **| tag}**

**no switchport trunk native vlan [tag]**

**Параметры**

| | |
|---|---|
| *VLAN-ID* | Native VLAN для trunk-порта. |
| **tag** | Включение режима тегирования 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 работает в режиме trunk mode. Когда native VLAN trunk-порта настроен в тегированном режиме (tagged mode), обычно допустимый тип кадров порта должен быть настроен как “tagged-only”, чтобы принимать только тегированные кадры. Когда trunk-порт работает в нетегированном режиме (untagged mode) для native VLAN, передавая нетегированный пакет для native VLAN и тегированные пакеты для всех остальных VLAN, допустимые типы кадров порта должны быть настроены как “admit-all” для корректной работы.

Указанная VLAN не должна обязательно существовать для настройки команды.

**Пример**

В данном примере показано, как настроить ethernet 1/0/1 в качестве интерфейса trunk и native VLAN 20.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 20
Switch(config-if)#
```

## *26.15. vlan*

Данная команда используется для добавления VLAN и входа в режим VLAN configuration mode. Используйте форму **no** для удаления VLAN.

**vlan** *VLAN-ID* **[, | -]**

**no vlan** *VLAN-ID* **[, | -]**

**Параметры**

| | |
|---|---|
| *VLAN-ID* | Идентификатор VLAN, которая должна быть добавлена, удалена или настроена. Корректный диапазон VLAN ID: от 1 до 4094. VLAN ID 1 не может быть удален. |
| **,** | (Опционально) Используется для перечисления нескольких VLAN или отделения одного диапазона номеров VLAN от предыдущего. Использование пробела до и после запятой недопустимо. |
| **-** | (Опционально) Используется для обозначения диапазона VLAN. Использование пробела до и после дефиса недопустимо. |

**По умолчанию**

VLAN ID 1 существует в системе в качестве VLAN по умолчанию.

**Режим ввода команды**

Global Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте команду **vlan** в режиме Global Configuration Mode для создания VLAN. Ввод команды **vlan** с VLAN ID обеспечивает вход в режим настройки VLAN (VLAN configuration mode). Ввод VLAN ID существующей VLAN не создает новую VLAN, но разрешает пользователю изменить параметры VLAN для указанной VLAN. Когда пользователь вводит VLAN ID новой VLAN, VLAN будет создана автоматически.

Используйте команду **no vlan** для удаления VLAN. VLAN по умолчанию не может быть удалена. Если удаленная VLAN является access VLAN порта, то access VLAN порта будет сброшена в VLAN 1.

**Пример**

В данном примере показано, как добавить новые VLAN, назначив новые VLAN с VLAN ID от 1000 до 1005.

```
Switch# configure terminal
Switch(config)# vlan 1000-1005
Switch(config-vlan)#
```

## *26.16. vlan precedence*

Данная команда используется для указания приоритета на порту на основе VLAN. Используйте форму **no** для сброса приоритета на порту на основе VLAN.

**vlan precedence {mac-vlan | subnet-vlan}**

**no vlan precedence**

**Параметры**

| | |
|---|---|
| **mac-vlan** | Классификация VLAN на основе MAC-адресов предпочтительней классификации VLAN на основе подсетей. |
| subnet-vlan | Классификация VLAN на основе подсетей предпочтительней классификации VLAN на основе MAC-адресов. |

**По умолчанию**

По умолчанию задана опция VLAN на основе MAC-адресов.

**Режим ввода команды**

Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

По умолчанию приоритет для классификации VLAN для нетегированного пакета является MAC-based > Subnet-based > Protocol VLAN. Используйте команду **vlan precedence** для настройки приоритета классификации VLAN между VLAN на основе MAC-адресов и VLAN на основе подсетей. Команда вступает в силу только для гибридных интерфейсов или интерфейсов dot1q tunnel.

**Пример**

В данном примере показано, как настроить ethernet 1/0/1 в качестве subnet VLAN, обладающей более высоким приоритетом.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# vlan precedence subnet-vlan
Switch(config-if)#
```

## *26.17. name*

Данная команда используется для указания имени VLAN. Используйте форму **no**, чтобы вернуть настройки по умолчанию.

**name** *VLAN-NAME*

**no name**

**Параметры**

| | |
|---|---|
| *VLAN-NAME* | Имя VLAN (макс. 32 символа). Имя VLAN должно быть уникальным в административном домене. |

**По умолчанию**

По умолчанию именем VLAN является VLANx, где x – четыре цифры номера VLAN, включая начальные нули.

**Режим ввода команды**

VLAN Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Используйте данную команду, чтобы задать имя VLAN. Имя VLAN должно быть уникальным в административном домене.

**Пример**

В данном примере показано, как задать имя “admin-vlan” для VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# name admin-vlan
Switch(config-vlan)#
```

## *26.18. counting*

Данная команда позволяет создать запись для сбора статистики на указанных интерфейсах L2 VLAN. Используйте форму **no**, чтобы удалить созданные записи.

**counting [interface** *INTERFACE-ID* **[,|-]] {broadcast | multicast |unicast | any} [rx | tx]**

**no counting [interface** *INTERFACE-ID* **[,|-]] [broadcast | multicast |unicast | any] [rx | tx]**

**Параметры**

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Опционально) Укажите один или несколько физических интерфейсов для подсчета трафика. Если физический интерфейс не указан, статистика ведется на основе каждой VLAN. |
| **,** | (Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Использование пробела до и после запятой недопустимо. |
| **-** | (Опционально) Используется для обозначения диапазона интерфейсов. Использование пробела до и после дефиса недопустимо. |
| **broadcast** | Указывается для подсчета широковещательных пакетов. |
| **multicast** | Указывается для подсчета пакетов многоадресной рассылки. |
| **unicast** | Указывается для подсчета одноадресных пакетов. |
| **any** | Указывается для подсчета всех пакетов независимо от типа. |
| **rx** | (Опционально) Указывается для подсчета входящего трафика. |
| **tx** | (Опционально) Указывается для подсчета исходящего трафика. |

**По умолчанию**

По умолчанию запись не указана.

**Режим ввода команды**

Layer 2 VLAN Interface Configuration Mode.

**Уровень команды по умолчанию**

Уровень 12.

**Использование команды**

Если тип кадров не указан, записи удаляются на основе интерфейсов и направления трафика. Если не указано направление трафика, подсчитывается и входящий, и исходящий трафик.

Данная команда применима только для интерфейса L2 VLAN и используется для продуктов с недостаточными для сбора статистики аппаратными ресурсами. Данный функционал может совместно использовать ресурсы ACL.

В параметре interface могут быть указаны только интерфейсы физических портов. Если интерфейс не указан, статистика собирается на основе VLAN. В качестве альтернативы подсчет ведется для указанного физического порта (-ов) в определенной VLAN.

Чтобы удалить все записи для определенных VLAN, используйте команду **no counting** без указания каких-либо параметров. Чтобы удалить все записи для конкретного физического порта (-ов) в конкретной VLAN, используйте команду **no counting interface** *INTERFACE-ID* **[,|-]** без указания остальных параметров.

**Пример**

В данном примере показано, как создать запись для подсчета входящего и исходящего трафика для VLAN 2.

```
Switch# configure terminal
Switch(config)# interface L2vlan 2
Switch(config-if)# counting any
Switch(config-if)#
```

В данном примере показано, как создать запись для подсчета входящих и исходящих широковещательных пакетов для VLAN 3.

```
Switch# configure terminal
Switch(config)# interface L2vlan 3
Switch(config-if)# counting broadcast
Switch(config-if)#
```

В данном примере показано, как создать запись для подсчета входящих одноадресных пакетов для физического интерфейса Ethernet 1/0/1 в VLAN 5.

```
Switch# configure terminal
Switch(config)# interface L2vlan 5
Switch(config-if)# counting interface ethernet 1/0/1 unicast rx
Switch(config-if)#
```

В данном примере показано, как удалить все записи для сбора статистики входящего и исходящего трафика для VLAN 2.

```
Switch# configure terminal
Switch(config)# interface L2vlan 2
Switch(config-if)# no counting all
Switch(config-if)#
```

В данном примере показано, как удалить все записи для сбора статистики входящего и исходящего трафика для физического интерфейса Ethernet 1/0/2 в VLAN 10.

```
Switch# configure terminal
Switch(config)# interface L2vlan 10
Switch(config-if)# no counting interface ethernet 1/0/2 all
Switch(config-if)#
```

В данном примере показано, как удалить все записи для сбора статистики исходящих многоадресных пакетов для физического интерфейса Ethernet 1/0/10 в VLAN 20.

```
Switch# configure terminal
Switch(config)# interface L2vlan 20
Switch(config-if)# no counting interface ethernet 1/0/10 multicast tx
Switch(config-if)#
```

## *26.19. show vlan counting*

Данная команда используется для отображения записей по сбору статистики на указанных интерфейсах L2 VLAN.

**show vlan counting [interface** *INTERFACE-ID***] [rx | tx]**

**Параметры**

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Опционально) Укажите один или несколько интерфейсов L2 VLAN для отображения информации о записях. Если интерфейс L2 VLAN |

| | |
|---|---|
| | не указан, то отображаются все созданные записи. |
| **rx** | (Опционально) Укажите, чтобы отобразить записи для входящего трафика. |
| **tx** | (Опционально) Укажите, чтобы отобразить записи для исходящего трафика. |

**По умолчанию**

Нет.

**Режим ввода команды**

User EXEC Mode.

Любой режим конфигурирования.

**Уровень команды по умолчанию**

Уровень 1.

**Использование команды**

Нет рекомендаций.

**Пример**

В данном примере показано, как получить информацию по всем записям сбора статистики на интерфейсах L2 VLAN.

```
Switch# show vlan counting

VLAN  Frame Type    Ports
----  ------------  -----------------------------------------------------
2     RX Unicast
3     RX Any
4     RX Multicast  1:1
10    RX Broadcast  1:1-1:5
2     TX Unicast
3     TX Any
4     TX Multicast  1:1
100   TX Broadcast  2:10-2:12

Total Entries: 8

Switch#
```