



T-KOM  
РОСАТОМ

# Руководство пользователя (CLI)

**Интеллектуальный управляемый коммутатор Gigabit Ethernet**

**Коммутаторы серии ТК-125**

Версия 1.0

Москва  
2022

# Содержание

<b>Содержание</b> .....	<b>2</b>
<b>1. Введение</b> .....	<b>4</b>
2. Базовые команды интерфейса командной строки .....	11
3. Команды 802.1X.....	22
4. Команды ACL (Список управления доступом) .....	36
5. Команды управления доступом .....	55
6. Команды предотвращения атак ARP Spoofing .....	70
7. Команды Asymmetric VLAN.....	72
8. Команды Authentication, Authorization и Accounting (AAA).....	73
9. Базовые команды настройки IPv4 .....	82
10. Базовые команды настройки IPv6 .....	88
11. Команды Cable Diagnostics.....	103
12. Команды Debug .....	107
13. Команды DHCP Auto-Configuration .....	111
14. Команды DHCP Client .....	114
15. Команды DHCP Relay .....	117
16. Команды DHCP Snooping .....	141
17. Команды DHCPv6 Client.....	161
18. Команды DHCPv6 Guard .....	163
19. Команды DHCPv6 Relay .....	167
20. Команды клиента D-Link Discovery Protocol (DDP) .....	183
21. Команды Domain Name System (DNS) .....	186
22. Команды предотвращения атак DoS .....	192
23. Команды Dynamic ARP Inspection .....	196
24. Команды Error Recovery.....	211
25. Команды File System .....	215
26. Команды Filter Database (FDB) .....	218
27. Команды Gratuitous ARP.....	231
28. Команды управления интерфейсом.....	232
29. Команды Internet Group Management Protocol (IGMP) Snooping.....	253
30. Команды IP-MAC-Port Binding (IMPB) .....	269
31. Команды многоадресной рассылки IP (IPMC).....	273
32. Команды IP Multicast версии 6 (IPMCv6).....	275
33. Команды IP Source Guard .....	277
34. Команды IP Utility.....	283
35. Команды IPv6 Snooping .....	286
36. Команды IPv6 Source Guard.....	291
37. Команды Jumbo Frame.....	296
38. Команды Link Aggregation Control Protocol (LACP) .....	298
39. Команды Link Layer Discovery Protocol (LLDP).....	305

40. Команды Loopback Detection (LBD) .....	335
41. Команды Mirror .....	341
42. Команды Multicast Listener Discovery (MLD) Snooping .....	345
43. Команды Multiple Spanning Tree Protocol (MSTP) .....	360
44. Команды Neighbor Discovery (ND) Inspection .....	370
45. Команды Network Access Authentication .....	374
46. Команды Network Protocol Port Protection .....	385
47. Команды Port Security .....	387
48. Команды Power over Ethernet (PoE) Commands (только для ТГК-125-24/4д-2П и ТГК-125-48/4д-2П) .....	394
49. Команды энергосбережения .....	414
50. Команды Protocol Independent .....	420
51. Команды качества обслуживания (QOS) .....	427
52. Команды Remote Network MONitoring (RMON) .....	452
53. Команды Router Advertisement (RA) Guard .....	460
54. Команды Safeguard Engine .....	464
55. Команды Secure Shell (SSH) .....	472
56. Команды уровня Secure Sockets Layer (SSL) .....	480
57. Команды протокола Simple Network Management Protocol (SNMP) .....	490
58. Команды Spanning Tree Protocol (STP) .....	513
59. Команды Storm Control .....	527
60. Команды Surveillance VLAN .....	532
61. Команды портов коммутатора .....	545
62. Команды управления системных файлов .....	550
63. Команды System Log .....	561
64. Команды времени и SNTP .....	569
65. Команды временного диапазона .....	576
66. Команды Traffic Segmentation .....	579
67. Команды Virtual LAN (VLAN) .....	581
68. Команды Voice VLAN .....	592
Приложение А - Записи системного журнала .....	600
Приложение Б. Записи trap-сообщений .....	623
Приложение В - Назначение атрибутов RADIUS .....	632
Приложение Г - Поддержка атрибутов IETF RADIUS .....	634

# 1. Введение

Описание команд в данном руководстве основано на версии программного обеспечения 2.01. Перечисленные здесь команды-это подмножество команд, поддерживаемых коммутатором серии ТГК-125. В описании используется интерфейс нашего технологического партнера, и некоторые надписи могут содержать названия и индексы, отличные от названий и индексов Т-КОМ. По мере выхода локализованного программного обеспечения, руководство будет корректироваться.

## Аудитория

Данное справочное руководство предназначено для сетевых администраторов и других специалистов по ИТ-сетям, ответственных за управление коммутатором с помощью интерфейса командной строки (CLI). CLI-это один из интерфейсов управления коммутатором серии ТГК-125, который в данном руководстве принято называть просто "коммутатор". Данное руководство написано с учетом того, что вы уже имеете опыт работы и знания в области Ethernet и современных принципов построения локальных сетей.

## Другая документация

Приведенные ниже документы являются дополнительным источником информации по настройке и устранению неисправностей коммутатора. Все документы доступны либо на компакт-диске, входящем в комплект поставки коммутатора, либо на веб-сайте Т-КОМ. Другие документы, относящиеся к данному коммутатору:

- Руководство по установке оборудования серии ТГК-125
- Справочное руководство по веб-интерфейсу серии ТГК-125

## Условные обозначения

Условное обозначение	Описание
<b>Полужирный шрифт</b>	Команды, параметры команд и ключевые слова печатаются жирным шрифтом. Ключевые слова в командной строке следует вводить точно так, как они отображаются.
<i>КУРСИВ ЗАГЛАВНЫМИ</i>	Параметры или значения, которые должны быть указаны, печатаются в <i>UPPERCASE ITALICS</i> . Параметры в командной строке должны быть заменены фактическими значениями, которые необходимо использовать в команде.
Квадратные скобки [ ]	Квадратные скобки заключают необязательное значение или набор необязательных аргументов.
Фигурные скобки { }	В скобках заключены альтернативные ключевые слова, разделенные вертикальными полосами. Как правило, можно выбрать одно из ключевых слов в разделенном списке.
Вертикальная линия	Необязательные значения или аргументы заключаются в квадратные скобки и разделяются вертикальными полосами. Как правило, можно выбрать одно или несколько значений или аргументов из разделенного списка.
Голубой шрифт Courier	Это соглашение используется для представления примера отображения консоли на экране, включая примеры ввода команд CLI с соответствующим выводом. Все примеры, используемые в данном руководстве, основаны на коммутаторе ТГК-125-48/4д-2П серии ТГК-125.

## Предупреждения

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



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



**Внимание:** информация о потенциальной угрозе устройству или о потере данных, а также способы это предотвратить.



**Предупреждение:** информация о потенциальной угрозе устройству или здоровью.

## Описания команд

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

- **Описание** – краткое описание функционала команды.
- **Синтаксис** – точная форма команды и правила ее написания.
- **Параметры** – таблица с кратким описанием опций или требуемых параметров и их использованием в команде.
- **По умолчанию** – если команда задает новое значение конфигурации или состояние коммутатора (например, отличное от используемого), это будет показано в данном поле.
- **Режим ввода команды** – режим, в котором возможно использование команды. Режимы описаны в разделе «Режимы ввода команд».
- **Уровень команды по умолчанию** – уровень привилегии пользователя, необходимый для использования команды.
- **Использование команды** – детальное описание команды и различных сценариев ее использования.
- **Пример** – пример использования команды в подходящем сценарии.

## Режимы ввода команд

В интерфейсе командной строки (CLI) доступно несколько режимов работы с командами. Набор команд, доступных пользователю, зависит от режима, в котором он находится в данный момент. Пользователь может увидеть все команды, доступные в определенном командном режиме, введя знак вопроса (?) в подсказке системы.

Интерфейс командной строки имеет несколько командных режимов. Существует два основных командных режима:

- User EXEC Mode
- Global Configuration Mode

Режимы специфической конфигурации доступны через **Global Configuration Mode**.

## EXEC Mode

Пользователи, вошедшие в систему в этом командном режиме, могут отслеживать всю информацию о системе и изменять любые параметры конфигурации системы, упомянутые в данном Руководстве по конфигурации.

## Global Configuration Mode

Основной целью режима глобальной конфигурации является применение глобальных настроек ко всему коммутатору. Помимо применения глобальных настроек ко всему коммутатору, пользователь может получить доступ к другим режимам настройки. Чтобы перейти в режим глобальной конфигурации, введите команду **configure terminal** в режиме EXEC.

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

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

Команда `exit` используется для выхода из режима глобальной конфигурации и возврата в режим EXEC.

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

Порядок действий для входа в специфические режимы представлен в дальнейших главах руководства. Режимы команд используются для конфигурации отдельных функций.

## Создание пользовательской учетной записи

Вы можете создавать различные учетные записи пользователей для различных уровней. Этот раздел поможет пользователю создать учетную запись пользователя с помощью интерфейса командной строки.



**Примечание:** По умолчанию на коммутаторе уже настроена одна учетная запись пользователя. Имя пользователя и пароль для этой учетной записи - `admin`.

Рассмотрим следующий пример.

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

В приведенном выше примере нам нужно было перейти и получить доступ к команде `username`.

- Мы ввели команду **configure terminal** для доступа к режиму глобальной конфигурации. Команда **username** может быть использована в режиме Global Configuration Mode.
- Команда **username account password account** создает учетную запись с именем пользователя *account* и паролем *account*.

Сохраните running configuration в start-up configuration. Это означает сохранение изменений, чтобы при перезагрузке коммутатора они не были утеряны. Следующий пример показывает, каким образом можно сохранить running configuration в start-up configuration.

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

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

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

Switch#
```

После перезагрузки коммутатора или выхода пользователя из учетной записи заданные имя пользователя и пароль должны быть введены для доступа к интерфейсу командной строки, как показано ниже.

```
DGS-1250-28XMP Gigabit Ethernet Smart Managed Switch

Command Line Interface
Firmware: Build 2.01.001
Copyright(C) 2020 D-Link Corporation. All rights reserved.

User Access Verification

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

## Сообщения об ошибке

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

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

Нижеследующий пример показывает, каким образом генерируется сообщение об ошибке Ambiguous command.

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

Нижеследующий пример показывает, каким образом генерируется сообщение об ошибке Incomplete command.

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

Нижеследующий пример показывает, каким образом генерируется сообщение об ошибке Invalid input detected.

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

## Функции редактирования

Интерфейс командной строки коммутатора поддерживает следующие клавиши для редактирования.

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

## Модификаторы отображения результатов вывода

Отображаемые результаты можно фильтровать с помощью команды **show** по следующим параметрам:

- **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.

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



```
Switch#show running-config | begin line console
line console
  session-timeout 0
!
line telnet
!
line ssh
!
protected-ports route-deny
!
ssh user admin authentication-method password
!
interface ethernet 1/0/1
  authentication host-mode multi-host
  ddp
!
interface ethernet 1/0/2
  authentication host-mode multi-host
  ddp
!
interface ethernet 1/0/3
  authentication host-mode multi-host
  ddp
!
interface ethernet 1/0/4
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

На примерах ниже показано использование параметра **include** *FILTER-STRING* в команде **show**.

```
Switch#show running-config | include Firmware
!                               Firmware: Build 2.01.001

Switch#
```

На примерах ниже показано использование параметра **exclude** *FILTER-STRING* в команде **show**.

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

Current configuration : 2654 bytes

line console
  session-timeout 0
line telnet
line ssh
protected-ports route-deny
ssh user admin authentication-method password
interface ethernet 1/0/1
  authentication host-mode multi-host
  ddp
interface ethernet 1/0/2
  authentication host-mode multi-host
  ddp
interface ethernet 1/0/3
  authentication host-mode multi-host
  ddp
interface ethernet 1/0/4
  authentication host-mode multi-host
  ddp
interface ethernet 1/0/5
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## 2. Базовые команды интерфейса командной строки

### 2-1 help

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

**help**

#### Параметры

Нет

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

Любой режим конфигурации

#### Использование команды

Команда help используется для отображения краткой справочной информации, включает следующие функции:

- Чтобы перечислить все доступные команды для определенного режима, введите вопросительный знак (?) в системную подсказку.
- Чтобы получить список команд, начинающихся с определенной строки символов, введите сокращенную команду, следующую сразу за вопросительным знаком (?). Такая форма называется **word help**, потому что она содержит только ключевые слова или аргументы, начинающиеся с введенного сокращения.
- Чтобы перечислить ключевые слова и аргументы, связанные с командой, введите вопросительный знак (?) на место ключевого слова или аргумента в командной строке. Такая форма называется **command syntax help**, потому что она содержит список ключевых слов или аргументов, применяемых на основе уже введенной команды, ключевого слова или аргументов.

#### Пример

В данном примере показано использование команды help для отображения краткого описания системы помощи.

```
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 **word** help для отображения команд режима Privileged EXEC, начинающихся с «re». Буквы, введенные после вопросительного знака (?) отпечатаны на следующей командной строке, чтобы позволить пользователю продолжить ввод команды.

```
Switch#re?
```

```
reset          renew          rename          reboot
```

```
Switch#re
```

В этом примере показано, как использовать **command syntax** help для отображения следующего аргумента частично завершенной команды **telnet**. Символы, введенные до знака вопроса (?), перепечатываются в следующей командной строке, чтобы пользователь мог продолжить ввод команды.

```
Switch#telnet ?
```

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

```
Switch#telnet
```

## 2-2 configure terminal

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

```
configure terminal
```

**Параметры**

Нет

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode.

#### Использование команды

Данная команда используется для входа в режим глобальной конфигурации

#### Пример

В данном примере показан процесс входа в режим глобальной конфигурации.

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

## 2-3 login (EXEC)

Данная команда используется для настройки имени пользователя.

### login

#### Параметры

Нет

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Данная команда используется для изменения имени пользователя учетной записи. Разрешено 3 попытки входа в интерфейс коммутатора. При использовании Telnet, если все попытки будут неудачными, доступ будет возвращен к командной строке. Если не введена никакая информация в течение 60 секунд, 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#
```

## 2-4 logout

Данная команда используется для закрытия активной сессии для выхода из коммутатора.

### logout

#### Параметры

Нет

По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Данная команда используется для закрытия активной сессии для выхода из коммутатора.

#### Пример

В данном примере показан процесс выхода.

```
Switch# logout
```

## 2-5 end

Данная команда используется для завершения текущего режима конфигурирования и возврата в самый верхний режим в иерархии режимов CLI, которым является режим EXEC.

### end

#### Параметры

Нет

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

Любой режим конфигурации

#### Использование команды

Данная команда используется для возвращения к высшему режиму в иерархии режимов CLI.

### Пример

В этом примере показано, как завершить режим конфигурации интерфейса и вернуться в режим EXEC Mode.

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

## 2-6 exit

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

### exit

#### Параметры

Нет

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

Любой режим конфигурирования

#### Использование команды

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

### Пример

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

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

## 2-7 show environment

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

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

<b>fan</b>	(Опционально) Отображение детальной информации о состоянии вентиляторов.
<b>power</b>	(Опционально) Отображение детальной информации о питании.
<b>temperature</b>	(Опционально) Отображение детальной информации о температуре.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

Любой режим конфигурирования

**Использование команды**

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

**Пример**

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

```
Switch# show environment

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

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

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

Switch#
```

**Отображаемые параметры**

<b>Power Module</b>	<b>Power 1:</b> питание переменным током (AC).
<b>Power Status</b>	<b>in-operation:</b> источник питания работает нормально.



---

**empty:** источник питания не подключен.

**failed:** силовой выпрямитель не работает нормально.

---

## 2-8 show unit

Данная команда позволяет получить общую информацию о системе.

**show unit**

### Параметры

Нет

**По умолчанию**

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте эту команду для отображения информации о модулях системы.

### Пример

В данном примере показано отображение информации о системных модулях (Units).

```
Switch#show unit
```

Model Descr		Model Name	
24P 10/100/1000M PoE + 4P 10G SFP+		DGS-1250-28XMP	
Serial-Number	Status	Up Time	
DGS1250102030	ok	0DT0H38M59S	
Memory	Total	Used	Free
DRAM	243268 K	125248 K	118020 K
FLASH	45220 K	24920 K	20300 K

```
Switch#
```

## 2-9 show cpu utilization

Данная команда позволяет получить информацию об использовании CPU.

**show cpu utilization**

### Параметры

Нет

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

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

### Пример

В данном примере показано получение информации о загрузке процессора.

```
Switch#show cpu utilization
CPU Utilization
Five seconds - 21 %      One minute - 22 %      Five minutes - 22 %
Switch#
```

## 2-10 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

EXEC Mode

### Использование команды

Используйте эту команду для отображения информации о версии коммутатора.

### Пример

В данном примере показано отображение информации о коммутаторе.

```
Switch#show version

System MAC Address: F0-7D-68-12-50-01

Module Name DGS-1250-28XMP
H/W A1
Runtime 2.01.001

Switch#
```

## 2-11 snmp-server enable traps environment

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

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

### Параметры

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

### По умолчанию

По умолчанию поддержка трапов для данных параметров отключена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

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

### Пример

В данном примере показан процесс включения трапов.

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

## 2-12 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 [high VALUE] [low VALUE]**  
**no environment temperature threshold [high] [low]**

### Параметры

<b>high</b>	(Опционально) Укажите верхнюю границу температуры в градусах Цельсия. Доступен диапазон от -100 до 200.
<b>low</b>	(Опционально) Укажите нижнюю границу температуры в градусах Цельсия. Доступен диапазон от -100 до 200. Нижняя граница не может быть выше верхней границы.

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### 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 этом примере показано, как настроить пороговые значения температуры окружающей среды.

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

## 2-13 show memory utilization

Эта команда используется для отображения информации об использовании памяти.

**show memory utilization**

### Параметры

Нет

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте эту команду для отображения информации об использовании памяти коммутатора, включая DRAM и флэш-память.

**Пример**

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

```
Switch#show memory utilization
```

Memory	Total	Used	Free
DRAM	243268 K	125316 K	117952 K
FLASH	45220 K	24968 K	20252 K

```
Switch#
```

## 3. Команды 802.1X

### 3-1 clear dot1x counters

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

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

#### Параметры

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

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

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

#### Пример

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

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

### 3-2 dot1x control-direction

Данная команда используется для настройки типа трафика на порту как однонаправленного (in) или двунаправленного (both). При использовании формы по команда вернет настройки по умолчанию.

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

## Параметры

<b>both</b>	Включение контроля трафика в двух направлениях.
<b>in</b>	Включение контроля трафика в одном направлении.

## По умолчанию

По умолчанию используется двунаправленный режим.

## Режим ввода команды

Interface Configuration Mode

## Использование команды

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

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

## Пример

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

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

## 3-3 dot1x default

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

### dot1x default

## Параметры

Нет

## По умолчанию

Аутентификация IEEE 802.1X отключена.  
 Двунаправленный режим потока.  
 Управление портом автоматическое.  
 Forward PDU на порту отключено.

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

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

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

#### Пример

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

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# 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 все к значениям по умолчанию.

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

#### Параметры

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

#### По умолчанию

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

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

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

Данная команда доступна только для конфигурации интерфейса физического порта. Если управление портом настроено как **force-authorized**, то контроль трафика в обоих направлениях не осуществляется.



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

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

### Пример

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

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

## 3-5 dot1x forward-pdu

Данная команда используется для включения функции продвижения кадров dot1x PDU. При использовании формы **no** данная команда отключит функцию продвижения кадров dot1x PDU.

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

### Параметры

Нет

### По умолчанию

По умолчанию данная опция отключена.

### Режим ввода команды

Interface Configuration Mode

### 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

<b>interface</b> INTERFACE-ID	Порт, на котором будет инициирована аутентификация. Доступными интерфейсами являются физические порты.
,	(Опционально) Используется для перечисления отдельных интерфейсов и их групп. Пробелы до и после запятой недопустимы.
-	(Опционально) Указывается для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы
<b>mac-address</b> MAC-ADDRESS	Указание MAC-адреса для инициализации.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

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

#### Пример

В данном примере показан процесс инициализации режима аутентификатора для Ethernet 1/0/1.

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

### 3-7 dot1x max-req

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

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

#### Параметры

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

#### По умолчанию

По умолчанию используется значение 2

#### Режим ввода команды

Interface Configuration Mode

#### 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 по данной команде отключит использование порта в качестве аутентификатора IEEE 802.1X.

**dot1x pae authenticator**  
**no dot1x pae authenticator**

#### Параметры

Нет

#### По умолчанию

Нет

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

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

#### Пример

В данном примере показан процесс конфигурации Ethernet 1/0/1 в качестве аутентификатора IEEE 802.1X PAE.

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

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

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

### 3-9 dot1x re-authenticate

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

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

#### Параметры

<b>interface</b> <i>INTERFACE-ID</i>	Указывает порт для повторной аутентификации. Доступными интерфейсами являются физические порты.
,	(Опционально) Используется для перечисления отдельных интерфейсов или групп интерфейсов. Пробелы до и после запятой недопустимы.
-	(Опционально) Указывается для обозначения диапазона интерфейсов. Пробелы до и после дефиса.
<b>mac-address</b> <i>MAC-ADDRESS</i>	Указание MAC-адреса для повторной аутентификации.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

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

#### Пример

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

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

### 3-10 dot1x system-auth-control

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

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

#### Параметры

Нет

#### По умолчанию

По умолчанию данная опция отключена.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

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

#### Пример

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

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

### 3-11 dot1x timeout

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

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

#### Параметры

<b>server-timeout SECONDS</b>	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.
<b>supp-timeout SECONDS</b>	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.
<b>tx-period</b> <i>SECONDS</i>	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

**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**

<b>interface</b> INTERFACE-ID	(Опционально) Интерфейс или группа интерфейсов, для которых будет отображаться конфигурация dot1x. Если значение не указано, отображаться будет глобальная конфигурация.
,	(Опционально) Используется для перечисления отдельных интерфейсов или групп интерфейсов. Пробелы до и после запятой недопустимы.
-	(Опционально) Указывается для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

**По умолчанию**

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

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

### Пример

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

```
Switch# show dot1x

802.1X                : Enabled
Trap State            : Enabled

Switch#
```

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

```
show dot1x interface eth1/0/1

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

Switch#
```

## 3-13 show dot1x diagnostics

Данная команда используется для просмотра результатов диагностики IEEE 802.1X.

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

### Параметры

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

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте эту команду для отображения диагностики 802.1X. Если параметр не указан, будет отображена информация обо всех интерфейсах.

**Пример**

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

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

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

Switch#
```

**3-14 show dot1x statistics**

Данная команда используется для просмотра статистики IEEE 802.1X.



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

#### Параметры

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

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

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

#### Пример

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

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

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

Switch#
```

### 3-15 show dot1x session-statistics

Данная команда используется для отображения статистики сессий IEEE 802.1X.

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

**Параметры**

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

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**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

### Использование команды

Используйте эту команду для включения или отключения отправки SNMP-уведомлений для аутентификации 802.1X.

### Пример

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

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

---

## 4. Команды ACL (Список управления доступом)

### 4-1 access-list resequence

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

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

#### Параметры

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

#### По умолчанию

Начальный порядковый номер по умолчанию – 10  
Значение шага по умолчанию – 10

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

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

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

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

#### Пример

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

```

Switch# configure terminal
Switch(config)# show access-list ip R&D

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

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

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

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

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

Switch(config)#

```

## 4-2 acl-hardware-counter

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

```

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

```

### Параметры

<b>access-group</b> ACCESS-LIST-NAME	Указывает имя настраиваемого списка доступа.
<b>access-group</b> ACCESS-LIST-NUMBER	Указывает номер конфигурируемого списка доступа.

### По умолчанию

По умолчанию эта опция отключена

### Режим ввода команды

Global Configuration Mode

### Использование команды

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

### Пример

В этом примере показано, как включить аппаратный счетчик ACL.

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

## 4-3 clear acl-hardware-counter

Эта команда используется для очистки аппаратного счетчика ACL.

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

### Параметры

<b>access-group</b>	Указывает группы доступа, которые необходимо очистить.
<i>ACCESS-LIST-NUMBER</i>	(Опционально) Указывает номер списка доступа, который необходимо очистить.
<i>ACCESS-LIST-NAME</i>	(Опционально) Укажите имя списка доступа, который необходимо очистить.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Если параметр не указан, все аппаратные счетчики группы доступа будут очищены.

### Пример

В этом примере показано, как очистить аппаратный счетчик ACL.

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

## 4-4 ip access-group

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

```
ip access-group {NAME | NUMBER} [in]
no ip access-group [NAME | NUMBER] [in]
```

### Параметры

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

### По умолчанию

Нет

### Режим ввода команды

Interface Configuration Mode

### Использование команды

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

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

### Пример

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

```
Switch# configure terminal
Switch(config)# interface eth1/0/2
Switch(config-if)#ip access-group Strict-Control
The remaining applicable IP related access entries are 704, remaining range entries are 16.
Switch(config-if)#
```

## 4-5 ip access-list

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

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

### Параметры

<b>extended</b>	(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.
<b>NAME</b>	Назначаемое имя списка доступа IP. Максимальное число допустимых символов в имени – 32.
<b>NUMBER</b>	Указывает идентификационный номер списка доступа IP. Для стандартных списков доступа IP это значение составляет от 1 до 1999. Для расширенных списков доступа IP это значение составляет от 2000 до 3999.

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

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

### Пример

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

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

## 4-6 ipv6 access-group

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

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



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

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

**По умолчанию**

Нет

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

К каждому интерфейсу можно применить только один список доступа определенного типа, но списки доступа различных типов могут быть применены к одному интерфейсу. Привязка группы доступа (access group) к интерфейсу будет расходовать ресурсы из записей фильтрации коммутатора. Если ресурсов недостаточно для активации команды, появится сообщение об ошибке.

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

**Пример**

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

```
Switch# configure terminal
Switch(config)# interface eth3/0/3
Switch(config-if)# ipv6 access-group ip6-control in
The remaining applicable IPv6 related access entries are 320, remaining range entries are 16.
Switch(config-if)#
```

**4-7 ipv6 access-list**

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

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

**Параметры**

<b>extended</b>	(Опционально) Указывает, что список доступа IPv6 является расширенным списком доступа IPv6 и есть возможность применить больше опций
-----------------	--

	фильтрации. Если параметр не указан, список доступа IPv6 будет считаться стандартным.
<i>NAME</i>	Назначаемое имя списка доступа IPv6. Максимальное число допустимых символов в имени – 32.
<i>NUMBER</i>	Указывает идентификационный номер списка доступа IPv6. Для стандартных списков доступа IPv6 это значение составляет от 11000 до 12999. Для расширенных списков доступа IPv6 это значение составляет от 13000 до 14999.

**По умолчанию**

Нет

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

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

**Пример**

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

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

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

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

**4-8 list remark**

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

```
list-remark TEXT
no list-remark
```

**Параметры**

<i>TEXT</i>	Указывает информацию о замечании. Длина информации может составлять до 256 символов.
-------------	--

**По умолчанию**

Нет

**Режим ввода команды**

Access-list Configuration Mode

**Использование команды**

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

**Пример**

В этом примере показано, как добавить примечание к списку доступа.

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

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

Switch#
```

**4-9 mac access-group**

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

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

**Параметры**

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

**По умолчанию**

Нет

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

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

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

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

**Пример**

В данном примере показано применение списка доступа MAC daily-profile к порту 4.

```
Switch# configure terminal
Switch(config)#interface eth1/0/4
Switch(config-if)#mac access-group daily-profile in
The remaining applicable MAC access entries are 204, remaining range entries are 32.
Switch(config-if)#
```

**4-10 mac access-list**

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

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

**Параметры**

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

**По умолчанию**

Нет

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Используйте данную команду, чтобы войти в режим MAC Access-List Configuration Mode, и введите команду **permit** или **deny**, чтобы указать записи. Имя каждого списка доступа должно быть уникальным. Все символы, используемые в имени, чувствительны к регистру. Если номер списка доступа не указан, автоматически будет назначен самый большой неиспользуемый номер из диапазона номеров списков доступа MAC.

### Пример

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

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

## 4-11 permit | deny (ip access-list)

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

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

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

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

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

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

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

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

```
rule [SEQUENCE-NUMBER] {permit | deny} {any | host SRC-IP-ADDR | SRC-IP-ADDR SRC-IP-WILDCARD}
[any | host DST-IP-ADDR | DST-IP-ADDR DST-IP-WILDCARD] [time-range PROFILE-NAME]
no SEQUENCE-NUMBER
```

### Параметры

<i>SEQUENCE-NUMBER</i>	Укажите порядковый номер. Доступен диапазон от 1 до 65535 Чем меньше номер, тем выше приоритет правила permit/deny.
<b>any</b>	Укажите IP-адрес источника или IP-адрес назначения.
<b>host SRC-IP-ADDR</b>	Укажите определенный IP-адрес узла источника.
<b>SRC-IP-ADDR SRC-IP-</b>	Укажите группу IP-адресов источника, используя значение wildcard.

<i>WILDCARD</i>	Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
<b>host</b> <i>DST-IP-ADDR</i>	Укажите определенный IP-адрес узла назначения.
<i>DST-IP-ADDR DST-IP- WILDCARD</i>	Укажите группу IP-адресов назначения, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
<b>precedence</b> <i>PRECEDENCE</i>	(Опционально) Укажите, чтобы пакеты могли фильтроваться по уровню приоритета (precedence). Доступны значения от 0 до 7.
<b>dscp</b> <i>DSCP</i>	(Опционально) Укажите DSCP-код для совпадений с заголовком IP. Доступен диапазон от 0 до 63, или выбор из следующих имен DSCP: af11 - 001010, af12 - 001100, af13 - 001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 - 110000, cs7 - 111000, default - 000000, ef - 101110.
<b>tos</b> <i>TOS</i>	(Опционально) Укажите, чтобы пакеты могли фильтроваться по уровню type of service. Доступны значения от 0 до 15
<b>lt</b> <i>PORT</i>	(Опционально) Укажите для сопоставления, если значение указанного порта меньше.
<b>gt</b> <i>PORT</i>	(Опционально) Укажите для сопоставления, если значение указанного порта больше.
<b>eq</b> <i>PORT</i>	(Опционально) Укажите для сопоставления, если значение указанного порта равно.
<b>neq</b> <i>PORT</i>	(Опционально) Укажите для сопоставления, если значение указанного порта не равно.
<b>range</b> <i>MIN-PORT MAX- PORT</i>	(Опционально) Укажите для сопоставления, если значение попадает в указанный диапазон портов.
<b>time-range</b> <i>PROFILE-NAME</i>	(Опционально) Укажите имя профиля периода времени, связанного со списком доступа, определяющим период его активации.
<b>tcp, udp, igmp, gre, esp, eigrp, ospf, rcp, pim, vrrp</b>	Укажите протоколы 4 уровня.
<i>PROTOCOL-ID</i>	(Опционально) Укажите Protocol ID. Доступен диапазон значений от 0 до 255.
<i>ICMP-TYPE</i>	(Опционально) Укажите тип сообщения ICMP. Доступны номера для типа сообщений от 0 до 255.
<i>ICMP-CODE</i>	(Опционально) Укажите код сообщения ICMP. Доступны номера для кода сообщений от 0 до 255.
<i>ICMP-MESSAGE</i>	(Опционально) Укажите сообщение ICMP. Для выбора доступны следующие предустановленные параметры: administratively-prohibited, alternate-address, conversion-error, host-prohibited, net-prohibited, echo, echo-reply, pointer-indicates-error, host-isolated, host-precedence-violation, host-redirect, host-tos-redirect, host-tos-unreachable, host-unknown, host-unreachable, information-reply, information-request, mask-reply, mask-request, mobile-redirect, net-redirect, net-tos-redirect, net-tos-unreachable, net-unreachable, net-unknown, bad-length, option-missing, packet-fragment, parameter-problem, port-unreachable, precedence-cutoff, protocol-unreachable, reassembly-timeout, redirect-message, router-advertisement, router-

---

solicitation, source-quench, source- route-failed, time-exceeded, timestamp-reply, timestamp- request, traceroute, ttl-expired, unreachable.

---

### По умолчанию

Нет

### Режим ввода команды

IP Access-list Configuration Mode

### Использование команды

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

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

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

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

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

### Пример

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

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

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

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

## 4-12 permit | deny (ipv6 access-list)

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

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

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

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

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

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

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

### Стандартный список доступа IPv6 (Standard IPv6 Access List):

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

**no** SEQUENCE-NUMBER

### Параметры

<i>SEQUENCE-NUMBER</i>	Укажите порядковый номер. Доступен диапазон от 1 до 65535 Чем меньше номер, тем выше приоритет правила permit/deny.
<b>any</b>	Укажите IPv6-адрес источника или IPv6-адрес назначения.
<b>host SRC-IPV6-ADDR</b>	Укажите определенный IPv6-адрес узла источника.
<i>SRC-IPV6-ADDR/PREFIX-LENGTH</i>	Укажите сеть IPv6 источника.
<b>host DST-IPV6-ADDR</b>	Укажите определенный IPv6-адрес узла назначения.
<i>DST-IPV6-ADDR/PREFIX-LENGTH</i>	Укажите сеть IPv6 назначения.



<b>tcp, udp, icmp, esp, pcp, sctp</b>	Укажите тип протокола 4 уровня.
<b>dscp</b> <i>VALUE</i>	(Опционально) Укажите совпадающее значение класса трафика в IPv6- хедере. Доступен диапазон от 0 до 63, или следующие DSCP-имена: af11 - 001010, af12 - 001100, af13 - 001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 - 110000, cs7 - 111000, default - 000000, ef - 101110.
<b>lt</b> <i>PORT</i>	(Опционально) Укажите для сопоставления, если значение указанного порта меньше.
<b>gt</b> <i>PORT</i>	(Опционально) Укажите для сопоставления, если значение указанного порта больше.
<b>eq</b> <i>PORT</i>	(Опционально) Укажите для сопоставления, если значение указанного порта равно.
<b>neq</b> <i>PORT</i>	(Опционально) Укажите для сопоставления, если значение указанного порта не равно.
<b>range</b> <i>MIN-PORT MAX-PORT</i>	(Опционально) Укажите для сопоставления, если значение попадает в указанный диапазон портов.
<i>PROTOCOL-ID</i>	(Опционально) Укажите Protocol ID. Доступен диапазон значений от 0 до 255.
<i>ICMP-TYPE</i>	(Опционально) Укажите тип сообщения ICMP. Доступны номера типа сообщений от 0 до 255.
<i>ICMP-CODE</i>	(Опционально) Укажите код сообщения ICMP. Доступны номера кода сообщений от 0 до 255.
<i>ICMP-MESSAGE</i>	(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.
<b>time-range</b> <i>PROFILE-NAME</i>	(Опционально) Укажите имя профиля периода времени, связанного со списком доступа, определяющим период его активации.
<i>TCP-FLAG</i>	(Опционально) Укажите поля TCP flag и указанные биты заголовка TCP с именем <b>ack</b> (acknowledge), <b>fin</b> (finish), <b>psh</b> (push), <b>rst</b> (reset), <b>syn</b> (synchronize) или <b>urg</b> (urgent).
<b>flow-label</b> <i>FLOW-LABEL</i>	(Опционально) Укажите значение Flow Label. Доступны значения от 0 до 1048575.
<b>fragments</b>	(Опционально) Укажите для фильтрации фрагментов пакета.

**По умолчанию**

Нет

**Режим ввода команды**

IPv6 Access-list Configuration Mode

## Использование команды

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

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

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

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

## Пример

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

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

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

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

## 4-13 permit | deny (mac access-list)

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

```
rule [SEQUENCE-NUMBER] {permit | deny} {any | host SRC-MAC-ADDR | SRC-MAC-ADDR SRC-MAC-
WILDCARD} {any | host DST-MAC-ADDR | DST-MAC-ADDR DST-MAC-WILDCARD} {ethernet-type TYPE MASK [cos
VALUE [inner INNER-COS]] [{vlan VLAN-ID} [inner INNER-VLAN]] [time-range PROFILE-NAME]
no SEQUENCE-NUMBER
```

**Параметры**

<i>SEQUENCE-NUMBER</i>	Укажите порядковый номер. Доступен диапазон от 1 до 65535 Чем меньше номер, тем выше приоритет правила permit/deny.
<b>any</b>	Укажите MAC-адрес источника или MAC-адрес назначения.
<b>host</b> <i>SRC-MAC-ADDR</i>	Укажите определенный MAC-адрес узла источника.
<i>SRC-MAC-ADDR SRC-MAC-WILDCARD</i>	Укажите группу MAC-адресов источника, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
<b>host</b> <i>DST-MAC-ADDR</i>	Укажите определенный MAC-адрес узла назначения.
<i>DST-MAC-ADDR DST-MAC-WILDCARD</i>	Укажите группу MAC-адресов назначения, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
<b>ethernet-type</b> <i>TYPE MASK</i>	(Опционально) Укажите тип Ethernet, являющийся шестнадцатеричным числом от 0 до FFFF или именем типа Ethernet. Доступны следующие имена: aarp, appletalk, decnet-iv, etype-6000, etype-8042, lat, lavc-sca, mop-console, mop-dump, vines-echo, vines-ip, xns-idp, arp.
<b>cos</b> <i>VALUE</i>	(Опционально) Укажите значение priority (приоритета) от 0 до 7.
<b>vlan</b> <i>VLAN-ID</i>	(Опционально) Укажите VLAN-ID.
<b>time-range</b> <i>PROFILE-NAME</i>	(Опционально) Укажите имя профиля периода времени, связанного со списком доступа, определяющим период его активации.

**По умолчанию**

Нет

**Режим ввода команды**

MAC Access-list Configuration Mode

**Использование команды**

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

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

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

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

В список может быть добавлено несколько записей, и вы можете использовать разрешение (permit) для одних, и запрет (deny) для других записей. Команды permit и deny могут соответствовать различным полям, доступным при настройке.

### Пример

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

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

## 4-14 show access-group

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

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

### Параметры

<b>interface INTERFACE-ID</b>	(Опционально) Укажите интерфейс, который необходимо отобразить.
-------------------------------	---

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

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

### Пример

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

```
Switch# show access-group

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

Switch#
```

## 4-15 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] | arp [NAME]]
```

### Параметры

<b>ip</b>	(Опционально) Укажите, чтобы отобразить все списки доступа IP.
<b>mac</b>	(Опционально) Укажите, чтобы отобразить все списки доступа MAC.
<b>ipv6</b>	(Опционально) Укажите, чтобы отобразить все списки доступа IPv6.
<b>NAME</b>	( Опциональн) Указывает имя списка доступа, который будет отображаться.
<b>NUMBER</b>	(Опционально) Указывает идентификатор списка доступа, который будет отображаться.
<b>arp</b>	Укажите, чтобы отобразить список доступа ARP.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Данная команда используется для отображения информации о списках доступа. Если не указана опция, будет отображен список всех настроенных списков доступа. Если указан тип списка доступа, будет отображена детальная информация о списке доступа. Если пользователь включит аппаратный счетчик ACL (ACL hardware counter) для списка доступа (access list) счетчик будет отображен на основе каждой записи списка доступа.

### Пример

В данном примере показано, как включить отображение всех списков доступа.

```
Switch# show access-list

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

Total Entries: 3

Switch#
```

В этом примере показано, как отобразить список доступа IP под названием "Strict-Control".

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

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

Switch#
```

В этом примере показано, как отобразить содержимое списка доступа, если его аппаратный счетчик включен.

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

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

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

Switch#
```

## 5. Команды управления доступом

### 5-1 access class

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

```
access-class IP-ACL
no access-class IP-ACL
```

#### Параметры

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

#### По умолчанию

Нет

#### Режим ввода команды

Line Configuration Mode

#### Использование команды

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

#### Пример

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

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

### 5-2 do

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

```
do COMMAND
```

#### Параметры

Нет

#### По умолчанию

Нет

#### Режим ввода команды

Любой режим конфигурации

#### Использование команды

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



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

#### Пример

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

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

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

В этом примере показано, как выполнить команду **show ip interface** в режиме глобальной конфигурации.

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

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

Total Entries: 1

Switch(config)#
```



## 5-3 ip http server

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

```
ip http server
no ip http server
```

### Параметры

Нет

### По умолчанию

По умолчанию данная опция включена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

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

### Пример

В данном примере показан процесс включения сервера HTTP.

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

## 5-4 ip http secure-server

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

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

### Параметры

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

### По умолчанию

По умолчанию данная опция отключена.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

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

**Пример**

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

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

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

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

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

**Параметры**

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

**По умолчанию**

Нет

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

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

**Пример**

В этом примере показано, как создается стандартный список доступа IP и указывается в качестве списка доступа для доступа к HTTP-серверу. Доступ к серверу разрешен только хосту 226.1.1.1.

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

## 5-6 ip http service-port

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

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

### Параметры

<i>TCP-PORT</i>	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

### Использование команды

Данная команда позволяет указать TCP-порт для сервера HTTP.

### Пример

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

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

## 5-7 ip http timeout-policy idle

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

```
ip http timeout-policy idle /NT
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

**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)#
```

## 5-8 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

**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)#
```

## 5-9 ip telnet service port

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

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

### Параметры

<i>TCP-PORT</i>	Номер порта TCP. Диапазон портов TCP: от 1 до 65535. Как правило, для Telnet назначается TCP-порт 23.
-----------------	---

### По умолчанию

По умолчанию используется порт 23.

### Режим ввода команды

Global Configuration Mode

### Использование команды

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

### Пример

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

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

## 5-10 line

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

```
line {console | telnet | ssh}
```

### Параметры

<b>console</b>	Локальная консольная сессия терминала.
<b>telnet</b>	Сессия терминала Telnet.
<b>ssh</b>	Сессия терминала SSH.

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

Данная команда позволяет войти в режим Line Configuration Mode.

### Пример

В данном примере 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)#
```

## 5-11 show terminal

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

**show terminal**

### Параметры

Нет

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### 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: 115200 bps

Switch#
```

## 5-12 show ip telnet server

Эта команда используется для отображения информации о состоянии сервера Telnet.

**show ip telnet server**

### Параметры

Нет

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте эту команду для отображения информации о состоянии сервера Telnet.

### Пример

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

```
Switch#show ip telnet server

Server State: Enabled

Switch#
```

## 5-13 show ip http server

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

**show ip http server**

### Параметры

Нет

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте эту команду для отображения информации о состоянии сервера HTTP.

**Пример**

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

```
Switch#show ip http server
ip http server state : Enabled
Switch#
```

## 5-14 show ip http secure-server

Данная команда используется для отображения информации о состоянии SSL.

**show ip http secure-server**

**Параметры**

Нет

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Данная команда используется для отображения информации о состоянии SSL.

**Пример**

В данном примере показан процесс отображения информации о состоянии SSL.



```
Switch# show ip http secure-server
ip http secure-server state : disable
Switch#
```

## 5-15 show users

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

**show users**

### Параметры

Нет

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Данная команда 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      Login-Time      IP address
-----
0    * console admin      25M58S
Total Entries: 1
Switch#
```

## 5-16 terminal length

Данная команда используется для настройки количества строк, отображаемых на экране. Команда **terminal length** влияет только на текущую сессию. Команда **terminal 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

<i>NUMBER</i>	Количество строк, отображаемое на экране. Допустимы значения от 0 до 512. При значении 0 отображение не прекратится, пока не будет достигнут конец отображаемого материала.
---------------	---

### По умолчанию

Значение по умолчанию – 24.

### Режим ввода команды

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

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

### Использование команды

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

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

За выводом от одной команды, выходящей за границу дисплея, будет следовать подсказка **–More–**. При появлении подсказки **–More–**, нажмите CTRL+C, q, Q или ESC, чтобы прервать вывод и вернуться к подсказке. Нажмите пробел для отображения дополнительного экрана вывода или нажмите Return для отображения еще одной строки вывода. При настройке длины экрана на 0 отключается функция прокручивания, из-за чего весь вывод экрана отображается сразу. Пока не будет использовано ключевое слово **default**, изменения значения **terminal length** будут применяться только к текущей сессии. При использовании формы **no** данной команды количество строк на экране терминала сбрасывается на 24.

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#
```

## 5-17 terminal speed

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

**terminal speed BPS**  
**no terminal speed**

**Параметры**

<i>BPS</i>	Скорость консоли в бит/с.
------------	---------------------------

**По умолчанию**

Значение по умолчанию – 115200.

**Режим ввода команды**

Global Configuration Mode

**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)#
```

**5-18 session-timeout**

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

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

**Параметры**

<i>MINUTES</i>	Тайм-аут в минутах. При использовании значения 0 тайм-аут не истекает никогда.
----------------	--

**По умолчанию**

Значение по умолчанию – 3 минуты.

**Режим ввода команды**

Line Configuration Mode

**Использование команды**

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

**Пример**

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

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

## 5-19 terminal width

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

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

### Параметры

<i>NUMBER</i>	Количество символов, отображаемое на экране. Допустимы значения от 40 до 255.
---------------	---

### По умолчанию

Значение по умолчанию – 80.

### Режим ввода команды

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

### Использование команды

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

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

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

### Пример

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

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

## 5-20 username

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

```
username NAME [noperword | password PASSWORD]
no username [NAME]
```

### Параметры

<i>NAME</i>	Указывает имя пользователя, состоящее максимум из 32 символов.
<b>noperword</b>	(Опционально) Указывает, что с этой учетной записью не будет связан пароль.
<b>password</b>	(Опционально) Укажите пароль для пользователя.
<i>PASSWORD</i>	(Опционально) Укажите строку пароля.

### По умолчанию

По умолчанию имя пользователя - *admin*, а пароль - *admin*.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Данная команда создает учетные записи пользователей. Когда пользователь войдет в систему, он окажется в режиме EXEC.

Если команда `no username` используется без указания имени пользователя, все пользователи удаляются.

Когда учетная запись пользователя пуста, пользователь будет находиться непосредственно в режиме EXEC.

### Пример

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

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

## 6. Команды предотвращения атак ARP Spoofing

### 6-1 ip arp spoofing-prevention

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

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

#### Параметры

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

#### По умолчанию

По умолчанию записей нет.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

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

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

Указать можно только физические порты.

#### Пример

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

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

## 6-2 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

### Использование команды

Данная команда используется для отображения всех записей ARP Spoofing Prevention.

### Пример

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

```
Switch# show ip arp spoofing-prevention

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

Total Entries: 1

Switch#
```

### Отображаемые параметры

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

## 7. Команды Asymmetric VLAN

### 7-1 asymmetric-vlan

Данная команда используется для запуска функции Asymmetric VLAN. Используйте форму **no**, чтобы отключить данную функцию.

```
asymmetric-vlan  
no asymmetric-vlan
```

#### Параметры

Нет

#### По умолчанию

По умолчанию данная функция отключена.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

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

#### Пример

В данном примере показано, как запустить функцию Asymmetric VLAN.

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

В этом примере показано, как отключить функцию Asymmetric VLAN.

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



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

### 8-1 aaa 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

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

#### По умолчанию

Метод аутентификации AAA не настроен.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте данную команду для настройки списка методов аутентификации по умолчанию для аутентификации 802.1X. Аутентификация запросов 802.1X будет выполняться на основе локальной базы данных.

#### Пример

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

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

## 8-2 aaa group server radius

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

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

### Параметры

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

### По умолчанию

Группа серверов AAA не настроена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте эту команду для определения группы серверов RADIUS. Определенная группа серверов может быть указана в качестве списка методов для аутентификации с помощью команды **aaa authentication**. Также используйте эту команду для входа в режим конфигурации сервера группы RADIUS. Используйте команду **server**, чтобы связать узлы сервера RADIUS с группой серверов RADIUS.

### Пример

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

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

## 8-3 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

**Использование команды**

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

**Пример**

В данном примере показано, как включить функцию AAA.

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

**8-4 clear aaa counters servers**

Данная команда используется для сброса счетчиков статистики серверов AAA.

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

**Параметры**

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

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

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

**Пример**

В данном примере показано, как сбросить счетчики серверов AAA.

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

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

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

**8-5 radius-server deadtime**

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

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

**Параметры**

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

**По умолчанию**

По умолчанию данным значением является 0.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

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

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

**Пример**

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

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

## 8-6 radius-server host

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

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

### Параметры

<i>IP-ADDRESS</i>	IP-адрес сервера RADIUS.
<i>IPV6-ADDRESS</i>	IPv6-адрес сервера RADIUS.
<b>auth-port</b> <i>PORT-NUMBER</i>	(Опционально) Номер UDP-порта назначения для отправки пакетов аутентификации. Диапазон: от 0 до 65535. Укажите ноль в качестве значения номера порта, если узел сервера не предназначен для аутентификации. Значение по умолчанию - 1812.
<b>timeout</b> <i>SECONDS</i>	Значение тайм-аута сервера. Диапазон: от 1 до 255 секунд. Если значение не указано, то значением по умолчанию является 5 секунд.
<b>retransmit</b> <i>COUNT</i>	(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.
<b>key</b> <i>KEY-STRING</i>	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

### Использование команды

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

### Пример

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

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

## 8-7 server (RADIUS)

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

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

### Параметры

<i>IP-ADDRESS</i>	IPv4-адрес сервера аутентификации.
<i>IPV6-ADDRESS</i>	IPv6-адрес сервера аутентификации.

### По умолчанию

По умолчанию сервер не настроен.

### Режим ввода команды

RADIUS Group Server Configuration Mode

### Использование команды

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

### Пример

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

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

## 8-8 show aaa

Данная команда используется для отображения глобального состояния AAA.

**show aaa**

### Параметры

Нет

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте эту команду для отображения глобального состояния AAA.

### Пример

В данном примере показано, как отобразить глобальное состояние AAA.

```
Switch# show aaa
AAA is enabled.
Switch#
```

## 8-9 show radius statistics

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

**show radius statistics**

### Параметры

Нет

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Уровень команды по умолчанию**

Уровень 1

**Использование команды**

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

**Пример**

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

```
Switch#show radius statistics

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

RADIUS Server: 172.19.11.20: Auth-Port 1600
State is Up
Auth.
Round Trip Time:      0
Access Requests:     0
Access Accepts:      0
Access Rejects:      0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

**Отображаемые параметры**



<b>Auth.</b>	Статистика для пакетов аутентификации
<b>Round Trip Time</b>	Интервал времени (в сотых долях секунды) между самым последним ответом и запросом, который соответствует ему, с этого сервера RADIUS.
<b>Access Requests</b>	Количество пакетов RADIUS Access-Request, отправленных на данный сервер. Не включает повторные передачи.
<b>Access Accepts</b>	Количество пакетов RADIUS Access-Accept (действительных или недействительных), полученных с данного сервера.
<b>Access Rejects</b>	Количество пакетов RADIUS Access-Reject (действительных или недействительных), полученных с данного сервера.
<b>Access Challenges</b>	Количество пакетов RADIUS Access-Challenge (действительных или недействительных), полученных с данного сервера.
<b>Retransmissions</b>	Количество пакетов RADIUS Request, повторно переданных данному серверу RADIUS. Повторные передачи включают записи, где идентификатор и Acct-Delay были обновлены, так же как и те, в которых они остаются одинаковыми.
<b>Malformed Responses</b>	Количество ошибочных пакетов RADIUS Response, полученных от данного сервера. Ошибочные пакеты включают пакеты с некорректной длиной. Неверные аутентификаторы, атрибуты Signature или неизвестные типы не включаются в ошибочные ответы.
<b>Bad Authenticators</b>	Количество пакетов RADIUS Response, содержащих некорректные аутентификаторы или атрибуты Signature, полученных от данного сервера.
<b>Pending Requests</b>	Количество пакетов RADIUS Request, предназначенных для данного сервера, время которых еще не истекло, или не получивших ответ. Эта переменная увеличивается, когда запрос отправляется, и уменьшается из-за приема ответа, тайм-аута или повторной передачи.
<b>Timeouts</b>	Количество тайм-аутов для данного сервера. После тайм-аута клиент может повторить попытку с тем же сервером, отправить другому серверу или отказаться. Повторная попытка с тем же сервером считается как повторная передача, а также как тайм-аут. Отправка другому серверу считается как запрос, а также как тайм-аут.
<b>Unknown Types</b>	Количество пакетов RADIUS неизвестного типа, полученных от данного сервера.
<b>Packets Dropped</b>	Количество пакетов RADIUS неизвестного типа, полученных от данного сервера и отброшенных по какой-либо причине.

## 9. Базовые команды настройки IPv4

### 9-1 arp

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

```
arp IP-ADDRESS HARDWARE-ADDRESS
no arp IP-ADDRESS HARDWARE-ADDRESS
```

#### Параметры

<i>IP-ADDRESS</i>	Укажите IP-адрес.
<i>HARDWARE-ADDRESS</i>	Укажите MAC-адрес (48-битный).

#### По умолчанию

В кэше ARP нет ни одной статической записи.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

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

#### Пример

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

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

### 9-2 arp timeout

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

```
arp timeout MINUTES
no arp timeout
```

#### Параметры

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

**По умолчанию**

По умолчанию установлено 240 минут.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

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

**Пример**

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

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

**9-3 clear arp-cache**

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

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

**Параметры**

<b>all</b>	Укажите, чтобы полностью очистить кэш динамических ARP-записей, связанных со всеми интерфейсами.
<i>INTERFACE-ID</i>	Укажите идентификатор интерфейса (Interface ID).
<i>IP-ADDRESS</i>	Укажите IP-адрес динамической ARP-записи, которую необходимо удалить.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

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

**Пример**

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

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

## 9-4 ip address

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

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

### Параметры

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

### По умолчанию

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

### Режим ввода команды

Interface Configuration Mode

### Использование команды

IPv4-адрес интерфейса может быть назначен вручную пользователем или динамически назначен DHCP-сервером. Используйте команду **no ip address** для удаления настроенной записи IP-адреса.



**Примечание:** Коммутатор поддерживает до четырех интерфейсов IPv4 и IPv6.

### Пример

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

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

## 9-5 show arp

Данная команда используется для отображения данных кэша ARP.

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

### Параметры

<i>ARP-TYPE</i>	(Опционально) Укажите тип ARP. <b>dynamic</b> – для отображения только динамических ARP-записей. <b>static</b> – для отображения только статических ARP-записей.
<i>ip-address</i> [ <i>MASK</i> ]	(Опционально) Укажите, если необходимо отобразить определенную запись или записи определенной сети.
<i>INTERFACE-ID</i>	(Опционально) Укажите, если необходимо отобразить ARP-записи, связанные с определенной сетью.
<i>HARDWARE-ADDRESS</i>	(Опционально) Укажите, если необходимо отобразить ARP-записи, чей аппаратный адрес равен данному MAC-адресу.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Данная команда позволяет отобразить информацию для определенной ARP-записи, всех ARP-записей, динамических или статических записей, а также для записей, связанных с определенным IP-интерфейсом.

### Пример

В данном примере показано, как отобразить данные кэша ARP.

```
Switch#show arp

S - Static Entry

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

Total Entries: 2

Switch#
```

## 9-6 show arp timeout

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

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

**Параметры**


---

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

---

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Данная команда используется для отображения заданного времени старения ARP-записей.

**Пример**

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

```
Switch#show arp timeout

Interface      Timeout (minutes)
-----
vlan1         60
-----

Total Entries:1

Switch#
```

**9-7 show ip interface**

Данная команда используется для отображения информации по IP-интерфейсу.

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

**Параметры**


---

<i>INTERFACE-ID</i>	(Опционально) Укажите, чтобы отобразить информацию по определенному IP-интерфейсу.
---------------------	--

---

<b>brief</b>	(Опционально) Укажите, чтобы отобразить информацию по IP-интерфейсу.
--------------	--

---

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

### Использование команды

Если параметр не указан, будет отображаться информация для всех интерфейсов.

### Пример

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

```
Switch#show ip interface brief

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

Total Entries: 1

Switch#
```

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

```
Switch#show ip interface vlan 1

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

Total Entries: 1

Switch#
```

## 10. Базовые команды настройки IPv6

### 10-1 clear ipv6 neighbors

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

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

#### Параметры

<b>all</b>	Укажите, чтобы удалить динамические записи из IPv6 neighbor cache для всех интерфейсов.
<b>interface <i>INTERFACE-ID</i></b>	Укажите, чтобы удалить динамические записи из IPv6 neighbor cache для конкретного интерфейса.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

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

#### Пример

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

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

### 10-2 ipv6 address

Данная команда используется для ручной настройки IPv6-адреса на интерфейсе. Используйте форму **no**, чтобы удалить заданный вручную IPv6-адрес.

```
ipv6 address {IPv6-ADDRESS/PREFIX-LENGTH | IPv6-ADDRESS link-local}
no ipv6 address {IPv6-ADDRESS/PREFIX-LENGTH | IPv6-ADDRESS link-local}
```

#### Параметры

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

#### По умолчанию



Нет

### Режим ввода команды

Interface Configuration Mode

### Использование команды

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

Интерфейсу можно назначить несколько IPv6-адресов, используя для этого различные механизмы, включая ручную настройку, настройку адресов без сохранения состояния (Stateless address configuration) и настройку адресов с сохранением состояния (Stateful address configuration).

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

### Пример

В данном примере показана настройка IPv6-адреса.

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

В данном примере показано, как удалить IPv6-адрес.

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

## 10-3 ipv6 address eui-64

Эта команда используется для настройки IPv6-адреса на интерфейсе с помощью идентификатора интерфейса EUI-64. Используйте форму **no** этой команды для удаления IPv6-адреса, сформированного с помощью идентификатора интерфейса EUI-64.

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

### Параметры

<i>IPV6-ADDRESS</i>	Указывает часть префикса IPv6 для настроенного IPv6-адреса.
<i>PREFIX-LENGTH</i>	Указывает длину префикса. Префикс адреса IPv6 также является локальной подсетью интерфейса. Длина префикса должна быть меньше 64.

**По умолчанию**

Нет

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Если команда настроена на туннель IPv6 ISTAP, последние 32 бита идентификатора интерфейса строятся с использованием IPv4-адреса источника туннеля.

**Пример**

В этом примере показано, как добавить адресную базу IPv6.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 address 3ffe:501:ffff:0::/64 eui-64
Switch(config-if)#
```

**10-4 ipv6 address dhcp**

Данная команда используется для настройки интерфейса на получение IPv6-адреса с помощью DHCPv6. Для отключения использования DHCPv6 на получение IPv6-адреса воспользуйтесь формой **no**.

```
ipv6 address dhcp [rapid-commit]
no ipv6 address dhcp
```

**Параметры**

<b>rapid-commit</b>	Укажите для получения адреса от сервера благодаря обмену двумя сообщениями. Опция rapid-commit будет указана в сообщении Solicit для запроса на подтверждение двумя сообщениями.
---------------------	--

**По умолчанию**

По умолчанию эта опция отключена.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Используйте эту команду для настройки интерфейса на получение параметров конфигурации сети IPv6 от сервера DHCPv6.

Стандартный обмен четырьмя сообщениями между DR и RR включает четыре сообщения: *SOLICIT*, *ADVERTISE*, *REQUEST* и *REPLY*. Если указан параметр **rapid-commit**, PP уведомит ДР в сообщении SOLICIT, что он может пропустить получение сообщения ADVERTISE и отправку сообщения REQUEST и перейти непосредственно к

получению сообщения REPLY от ДР, чтобы завершить обмен двумя сообщениями вместо стандартного обмена четырьмя сообщениями. Сообщение REPLY содержит параметры конфигурации сети.

Для правильной работы параметр **rapid-commit** должен быть включен как на DR, так и на RR.

При использовании команды по существующие параметры конфигурации сети IPv6, полученные от сервера DHCPv6, будут сохранены. DHCPv6-сервера, будут удалены.

### Пример

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

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

## 10-5 ipv6 enable

Данная команда используется для включения обработки IPv6 на интерфейсах, у которых нет явно настроенного IPv6-адреса. Используйте форму **no**, чтобы отключить обработку IPv6 на интерфейсах, у которых нет явно настроенного IPv6-адреса.

**ipv6 enable**  
**no ipv6 enable**

### Параметры

Нет

### По умолчанию

Данная опция по умолчанию отключена.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

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

### Пример

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

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

## 10-6 ipv6 hop-limit

Данная команда используется для настройки параметра Hop Limit (предельное число шагов) для IPv6 на коммутаторе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ipv6 hop-limit VALUE
no ipv6 hop-limit
```

### Параметры

VALUE	Укажите диапазон значений для параметра IPv6 Hop Limit. Если задан 0, для отправки пакета используются настройки по умолчанию. Допустимые значения: от 0 до 255.
-------	--

### По умолчанию

Значение по умолчанию – 64.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Используйте данную команду для настройки параметра Hop Limit, который будет анонсироваться в сообщениях RA. Пакет IPv6, сгенерированный в системе, также будет использовать это значение в качестве начального значения параметра Hop Limit.

### Пример

В этом примере показано, как настроить значение ограничения IPv6 hop limit на 255.

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

## 10-7 ipv6 nd managed-config-flag

Данная команда используется для включения флага Managed Configuration (M) в анонсируемых сообщениях RA. Для выключения флага используйте форму **no**.

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

### Параметры

Нет

### По умолчанию

Данный функционал по умолчанию отключен.

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

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

#### Пример

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

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

## 10-8 ipv6 nd other-config-flag

Данная команда используется для включения флага Other Configuration (O) в анонсируемых сообщениях RA. Для выключения флага используйте форму **no**.

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

#### Параметры

Нет

#### По умолчанию

Данный функционал по умолчанию отключен.

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

Когда эта функция включена, маршрутизатор будет инструктировать подключенные узлы использовать протокол конфигурации с состоянием для получения информации об автоконфигурации, отличной от адреса IPv6.

#### Пример

В этом примере показано, как включить флаг IPv6 other configure в RA, рекламируемых в VLAN 1.

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

## 10-9 ipv6 nd prefix

Данная команда используется для настройки IPv6-префикса, который будет анонсироваться в сообщениях RA. Для удаления префикса используйте форму **no**.

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

### Параметры

<i>IPV6-PREFIX</i>	Введите здесь префикс IPv6, который будет создан или рекламироваться в RA на интерфейсе.
<i>PREFIX-LENGTH</i>	Введите здесь длину префикса IPv6, который будет создан или рекламироваться в RA на интерфейсе.
<i>VALID-LIFETIME</i>	(Опционально) Введите здесь действительное значение времени жизни. Диапазон составляет от 0 до 4294967295 секунд.
<i>PREFERRED-LIFETIME</i>	(Опционально) Введите здесь предпочтительное значение времени жизни. Диапазон составляет от 0 до 4294967295 секунд.
<b>off-link</b>	(Опционально) Указывает на отключение флага включения.
<b>no-autoconfig</b>	(Опционально) Указывает на отключение флага автоконфигурации.

### По умолчанию

По умолчанию допустимое значение времени жизни составляет 2592000 секунд (30 дней).

Предпочтительное значение времени жизни по умолчанию - 604800 секунд (7 дней).

По умолчанию флаг отключения и флаг автоконфигурации включен.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Для префикса допустимое время жизни должно быть больше, чем предпочтительное время жизни. Они имеют смысл, если у префикса включен бит A. Полученный узел выполнит конфигурацию адреса без статического состояния на основе префикса. Если время жизни префикса превысило предпочтительное время жизни, то IPv6-адрес, сконфигурированный на основе этого префикса, перейдет в состояние deprecated. Если время жизни префикса превысило допустимое время жизни, то IPv6-адрес, сконфигурированный на основе этого префикса, будет удален.

Если IPv6-адрес сконфигурирован на интерфейсе вручную, соответствующий префикс будет автоматически рекламироваться. Рекламируемый префикс можно изменить, но нельзя удалить с помощью этой команды.

Если IPv6-адрес будет удален позже, реклама соответствующего префикса также будет остановлена.

### Пример

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

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

## 10-10 ipv6 nd ra interval

Данная команда используется для настройки временного интервала между сообщениями RA для IPv6-интерфейса.

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

### Параметры

<i>MAX-SECS</i>	Укажите максимальный временной интервал для повторной передачи сообщения RA (в секундах). Допустимые значения: от 4 до 1800 секунд.
<i>MIN-SECS</i>	(Опционально) Укажите минимальный временной интервал для повторной передачи сообщения RA (в секундах). Допустимые значения: от 3 до 1350 секунд

### По умолчанию

Максимальный временной интервал по умолчанию – 200 секунд.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Следующие правила применяются к минимальному значению интервала RA, если минимальное значение не настроено:

- Если максимальное значение интервала RA равно или больше 9 секунд, то минимальное значение будет составлять 33% от максимального значения.
- Если максимальное значение интервала RA меньше 9 секунд, то минимальное значение будет равно максимальному значению.

### Пример

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

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

## 10-11 ipv6 nd ra lifetime

Данная команда используется для настройки значения времени жизни (Lifetime) в анонсируемых сообщениях RA. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

#### Параметры

<b>SECONDS</b>	Укажите время жизни для использования маршрутизатора в качестве маршрутизатора по умолчанию (в секундах). Допустимые значения: от 0 до 9000.
----------------	---

#### По умолчанию

Значение по умолчанию – 1800 секунд.

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

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

#### Пример

В этом примере показано, как настроить значение времени жизни, рекламируемое в RA, на 9000 секунд.

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

## 10-12 ipv6 nd suppress-ra

Данная команда используется для отключения отправки сообщений RA на интерфейсе. Для включения отправки сообщений RA используйте форму **no**.

**ipv6 nd suppress-ra**  
**no ipv6 nd suppress-ra**

#### Параметры

Нет

#### По умолчанию

По умолчанию эта функция включена на интерфейсе VLAN и отключена на туннельном интерфейсе.

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды



Используйте эту команду, чтобы отключить отправку RA-сообщений на интерфейсе. Используйте команду `no` для повторно включить отправку RA-сообщений на туннельном интерфейсе ISATAP.

### Пример

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

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

## 10-13 ipv6 nd reachable-time

Данная команда используется для настройки параметра Reachable Time (время доступности) в таблице ND-протокола. Используйте форму `no`, чтобы вернуться к настройкам по умолчанию.

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

### Параметры

<i>MILLI-SECONDS</i>	Введите здесь время досягаемости, используемое в протоколе ND. Диапазон от 0 до 3600000 миллисекунд с кратностью 1000 миллисекунд.
----------------------	--

### По умолчанию

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

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Заданное время используется маршрутизатором на интерфейсе и анонсируется в сообщении RA. Если задан 0, маршрутизатор будет использовать 30 секунд на интерфейсе и анонсировать 0 (не указано) в сообщении RA.

Параметр Reachable Time используется IPv6-узлом для определения доступности соседних узлов.

### Пример

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

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

## 10-14 ipv6 nd ns-interval

Данная команда используется для настройки временного интервала между повторными отправлениями сообщений NS. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

#### Параметры

<i>MILLI-SECONDS</i>	Укажите временной интервал между отправлениями запросов NS (в миллисекундах). Допустимые значения: от 0 до 3600000 миллисекунд, кратно 1000.
----------------------	--

#### По умолчанию

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

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

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

#### Пример

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

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

## 10-15 ipv6 neighbor

Данная команда используется для создания статической записи в таблице IPv6 neighbor. Используйте форму **no**, чтобы удалить статическую запись из таблицы.

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

#### Параметры

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

#### По умолчанию

Нет

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте эту команду для создания статической записи кэша соседей IPv6 на интерфейсе. Статическая запись будет находиться либо в состоянии REACHABLE, если интерфейс UP, либо в состоянии INCOMPLETE, если интерфейс down. Процесс обнаружения достижимости не будет применяться к статическим записям.

Команда **clear ipv6 neighbors** очистит записи кэша динамических соседей. Используйте команду **no ipv6 neighbor** для удаления записи статического соседа.

#### Пример

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

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

## 10-16 show ipv6 interface

Данная команда используется для просмотра информации по IPv6-интерфейсу.

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

#### Параметры

<i>INTERFACE-ID</i>	(Опционально) Укажите интерфейс для получения информации по нему.
<b>brief</b>	(Опционально) Укажите, чтобы получить краткую информацию.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте эту команду для отображения конфигураций, связанных с интерфейсом IPv6.

#### Пример

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

```
Switch#show ipv6 interface vlan2

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

Total Entries: 1

Switch#
```

В 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#
```

## 10-17 show ipv6 neighbors

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

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

**Параметры**

<i>INTERFACE-ID</i>	Укажите интерфейс для отображения информации о записях в таблице IPv6 neighbor cache.
<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес, чтобы получить для него информацию о записях в таблице IPv6 neighbor cache.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

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

**Пример**

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

```
Switch# show ipv6 neighbors
```

```
IPv6 Address                               Link-Layer Addr  Interface Type State
-----
FE80::200:11FF:FE22:3344                  00-00-11-22-33-44 vlan1      D   REACH
```

```
Total Entries: 1
```

```
Switch#
```

**Отображаемые параметры**

<b>Тип записи</b>	<b>D</b> – динамическая изученная запись. <b>S</b> – статическая neighbor-запись.
<b>Состояние записи</b>	<b>INCOMPLETE</b> (неполное) – состояние, когда запрос на получение адреса для записи отправлен, но ответное сообщение Neighbor Advertisement еще не получено. <b>REACH</b> (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. <b>STALE</b> – состояние, в которое переходит запись, если с момента получения последнего подтверждения прошло больше заданного таймером Reachable Time времени (в миллисекундах). <b>PROBE</b> – состояние записи, при котором устройство отправляет сообщение Neighbor Solicitation, чтобы подтвердить достижимость. <b>DELAY</b> - neighbor больше не считается достижимым, и

---

недавно на него был отправлен трафик. Вместо немедленного зондирования neighbor отложите отправку зондов на некоторое время, чтобы дать протоколам верхнего уровня возможность подтвердить достижимость.

---

## 11. Команды Cable Diagnostics

### 11-1 test cable-diagnostics

Данная команда используется для запуска диагностики кабеля, предполагающей анализ состояния и длины медных кабелей.

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

#### Параметры

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

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Данная команда используется для настройки физических портов. Диагностика кабеля позволяет выявить проблемы с подключением на медных портах. Для запуска диагностики используйте команду **test cable-diagnostics**. Медный порт может находиться в одном из следующих состояний:

- **Open:** кабель не подключен к ответному устройству.
- **Short:** замыкание в одной паре кабеля.
- **Open or Short:** кабель не подключен к ответному устройству или обнаружено замыкание в одной паре кабеля, но PHY не удается распознать тип неисправности.
- **Crosstalk:** замыкание между разными парами кабеля.
- **Shutdown:** удаленный партнер отключен.
- **Unknown:** неизвестное состояние диагностики кабеля.
- **OK:** неисправностей витой пары/кабеля не выявлено.
- **No cable:** на порту отсутствует подключение к удаленному партнеру.

#### Пример

В данном примере показано, как запустить диагностику кабеля для анализа статуса и длины медных кабелей.

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

## 11-2 show cable-diagnostics

Данная команда используется для просмотра результатов диагностики кабеля.

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

### Параметры

<b>interface</b> INTERFACE-ID	(Опционально) Укажите ID интерфейса. Допустимым интерфейсом является физический порт.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Эта команда доступна только для конфигурации интерфейса физического порта. Используйте эту команду для отображения результатов тестирования для диагностики кабеля.

### Пример

Просмотр результатов диагностики кабеля.



```
Switch# show cable-diagnostics

Port      Type      Link Status  Test Result      Cable Length (M)
-----
eth1/0/1  1000BASE-T Link Up      Pair 1 Open     at 0M -
          Pair 2 OK      at 7M
          Pair 3 OK      at 7M
          Pair 4 Open     at 0M
eth1/0/2  1000BASE-T Link Down    -               -
eth1/0/3  1000BASE-T Link Down    -               -
eth1/0/4  1000BASE-T Link Down    -               -
eth1/0/5  1000BASE-T Link Down    -               -
eth1/0/6  1000BASE-T Link Down    -               -
eth1/0/7  1000BASE-T Link Down    -               -
eth1/0/8  1000BASE-T Link Down    -               -
eth1/0/9  1000BASE-T Link Down    -               -
eth1/0/10 1000BASE-T Link Down    -               -
eth1/0/11 1000BASE-T Link Down    -               -
eth1/0/12 1000BASE-T Link Down    -               -
eth1/0/13 1000BASE-T Link Down    -               -
eth1/0/14 1000BASE-T Link Down    -               -
eth1/0/15 1000BASE-T Link Down    -               -
eth1/0/16 1000BASE-T Link Down    -               -
eth1/0/17 1000BASE-T Link Down    -               -
eth1/0/18 1000BASE-T Link Down    -               -
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

### 11-3 clear cable-diagnostics

Данная команда используется для очистки результатов диагностики кабеля.

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

#### Параметры

<b>all</b>	Используется для очистки результатов диагностики кабеля для всех интерфейсов.
<b>interface <i>INTERFACE-ID</i></b>	Укажите идентификатор интерфейса.
<b>,</b>	(Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
<b>-</b>	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

#### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Эта команда доступна только для конфигурации интерфейса физического порта. Используйте эту команду для очистки результатов тестирования для диагностики кабеля. Если тест запущен на интерфейсе, будет выведено сообщение об ошибке.

### Пример

В данном примере показано, как очистить результаты диагностики кабеля.

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

## 12. Команды Debug

### 12-1 debug reboot on-error

Данная команда используется для включения режима перезапуска коммутатора при возникновении критических ошибок. Используйте форму **no**, чтобы отключить режим перезапуска при возникновении критических ошибок.

```
debug reboot on-error
no debug reboot on-error
```

#### Параметры

Нет

#### По умолчанию

По умолчанию данный режим включен.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

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

#### Пример

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

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

### 12-2 debug copy

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

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

#### Параметры

---

*SOURCE-URL*

Укажите ссылку на файл, который необходимо скопировать:  
**error-log:** укажите, чтобы скопировать данные журнала регистрации ошибок.

---

---

	<b>tech-support:</b> укажите, чтобы скопировать справочную техническую информацию.
<i>LOCATION</i>	Укажите адрес IPv4 или IPv6 TFTP-сервера.

---

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте данную команду для копирования информации по отладке в указанный файл.

**Пример**

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

```
Switch# debug copy tech-support tftp: //10.90.90.99/abc.txt

Address of remote host [10.90.90.99]?
Destination filename [abc.txt]?
Connecting to server..... Done.
Upload tech-support..... 100 %

Success.

Switch#
```

### 12-3 debug clear error-log

Данная команда используется для очистки журнала регистрации ошибок.

**debug clear error-log**

**Параметры**

Нет

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

### Использование команды

Используйте данную команду для очистки журнала регистрации ошибок.

### Пример

В данном примере показано, как очистить журнал регистрации ошибок.

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

## 12-4 debug show error-log

Данная команда используется для отображения данных журнала регистрации ошибок.

**debug show error-log**

### Параметры

Нет

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте данную команду для отображения данных журнала регистрации ошибок.

### Пример

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

```

Switch#debug show error-log
Exception signal 11 caught: Segmentation fault
Address: 0
Task: 0x023CCA78 "CLI"
Stack Usage (used max/size): 9320/196608 bytes
Registers:
    pc=00000000
    $0=00000000    $1(at)=00000001    $2(v0)=00000000    $3(v1)=00000074
$4(a0)=00000000    $5(a1)=014FFB15    $6(a2)=00000000    $7(a3)=00000000
$8(t0)=00000064    $9(t1)=00000064    $10(t2)=0018F730    $11(t3)=FFFFFFFE
$12(t4)=02406EB8    $13(t5)=73947BC8    $14(t6)=20000000    $15(t7)=00000074
$16(s0)=68173794    $17(s1)=739503B8    $18(s2)=738404F0    $19(s3)=6817379C
$20(s4)=00000001    $21(s5)=6FB45D3C    $22(s6)=00000004    $23(s7)=68173928
$24(t8)=00CF81C4    $25(t9)=00D60E10    $26(k0)=68174524    $27(k1)=00000000
$28(gp)=016F7B70    $29(sp)=681736E0    $30(fp)=016FCCB4    $31(ra)=00D15A30
Back Trace (for reference only):
->00D15A28
->023AF920
->00D60E20 strcpy+0X10/0X24
Stack:
681736E0  739503B8 738404F0 68173798 00000001  s...s...h.7.....
681736F0  016F7B70 016FCCB4 68173928 00195818  .o(p.o..h.9(..X.
68173700  778C2020 00000000 000030D4 023AF928  w. ....0...:(
68173710  00000001 00000000 00000000 00000000  .....
68173720  016FCCB4 00000000 00000000 2F000004  .o...../...
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All

```

## 12-5 debug show tech-support

Эта команда используется для отображения информации, необходимой персоналу технической поддержки.

### debug show tech-support

#### Параметры

Нет

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте эту команду для отображения информации технической поддержки. Информация технической поддержки используется для сбора информации о коммутаторе, необходимой инженерам для устранения неполадок или анализа проблемы.

### Пример

В данном примере показано, как отобразить информацию о технической поддержке всех модулей.

```
Switch#debug show tech-support

#-----
#           DGS-1250-28XMP Gigabit Ethernet Smart Managed Switch
#           Technical Support Information
#
#           Firmware: Build 2.01.001
#   Copyright (C) 2020 D-Link Corporation. All rights reserved.
#-----

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

[SYS 2000-1-1 00:12:25]

Boot Time       : 1 Jan 2000  00:00:00
RTC Time        : 2000/01/01 00:12:25
Bootloader Version : 3.3.0.31-12
Linux Version    : 3.18.24-18 #3 Mon Mar 25 22:31:47 CST 2019
Runtime Version  : 2.01.001
Hardware Version  : A1
Serial number    : DGS1250102030
MAC Address      : F0-7D-68-12-50-01
MAC Address Number : 28

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

## 13. Команды DHCP Auto-Configuration

### 13-1 autoconfig enable

Данная команда используется для включения функции автоконфигурации. Используйте форму **no**, чтобы отключить данную функцию.

**autoconfig enable**  
**no autoconfig enable**

#### Параметры

Нет

### По умолчанию

По умолчанию данная функция выключена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

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

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

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

### Пример

В данном примере показано, как включить автоконфигурацию.

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

## 13-2 show autoconfig

Данная команда используется для отображения статуса автоконфигурации.

```
show autoconfig
```

### Параметры

Нет

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды



Данная команда используется для отображения статуса автоконфигурации.

### **Пример**

В данном примере показано, как отобразить статус автоконфигурации.

```
Switch# show autoconfig  
  
Autoconfig State: Disabled  
  
Switch#
```

## 14. Команды DHCP Client

### 14-1 ip dhcp client class-id

Данная команда используется для обозначения Vendor Class Identifier, используемого в качестве значения Option 60 для сообщения DHCP Discover. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip dhcp client class-id {STRING | hex HEX-STRING}
no ip dhcp client class-id
```

#### Параметры

<i>STRING</i>	Укажите Vendor Class Identifier в формате строки. Максимальная длина строки – 32 символа.
<i>HEX-STRING</i>	Укажите Vendor Class Identifier в шестнадцатеричном формате. Максимальная длина строки – 64 символа.

#### По умолчанию

По умолчанию в качестве ID класса используется тип устройства.

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

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

#### Пример

В данном примере показано, как включить DHCP-клиент, запустить отправку Vendor Class Identifier и указать его значение. Указанное значение – VOIP-Device для VLAN 100.

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

### 14-2 ip dhcp client client-id

Данная команда используется для обозначения интерфейса VLAN, чей шестнадцатеричный MAC-адрес будет использован в качестве ID клиента, отправляемого в сообщении Discover. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

#### Параметры

<i>INTERFACE-ID</i>	Укажите интерфейс VLAN, чей шестнадцатеричный MAC-адрес будет использован в качестве ID клиента и отправлен в сообщении Discover.
---------------------	---

#### По умолчанию

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

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

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

#### Пример

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

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

### 14-3 ip dhcp client lease

Данная команда используется для указания времени аренды IP-адреса, который необходимо запросить у DHCP-сервера. Используйте форму **no**, чтобы отключить данную функцию.

```
ip dhcp client lease DAYS [HOURS [MINUTES]]
no ip dhcp client lease
```

#### Параметры

<i>DAYS</i>	Укажите продолжительность аренды в днях. Допустимый диапазон: от 0 до 10000 дней.
<i>HOURS</i>	(Опционально) Укажите продолжительность аренды в часах.

---

	Допустимый диапазон: от 0 до 23 часов.
<i>MINUTES</i>	(Опционально) Укажите продолжительность аренды в минутах. Допустимый диапазон: от 0 до 59 минут.

---

#### По умолчанию

Время аренды не запрашивается.

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

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

#### Пример

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

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

## 15. Команды DHCP Relay

### 15-1 class (DHCP Relay)

Эта команда используется для входа в режим конфигурации пула DHCP и ассоциации диапазона IP-адресов с классом DHCP. Для удаления ассоциации используйте форму **no** этой команды.

```
class NAME
no class NAME
```

#### Параметры

<i>NAME</i>	Указывает имя класса DHCP с максимальным количеством символов 32.
-------------	---

#### По умолчанию

Нет

#### Режим ввода команды

DHCP Pool Configuration Mode

#### Использование команды

Эта команда используется для связывания пула ретрансляции DHCP с классом пула DHCP. Используйте команду **relay target** для определения списка целевых адресов ретрансляции для пересылки пакетов DHCP. Если запрос клиента DHCP соответствует пулу ретрансляции, который настроен с классами, клиент должен соответствовать классу, настроенному в пуле, чтобы быть переданным. Если класс DHCP не настроен, запрос будет сопоставлен только с пулом ретрансляции и будет передан на сервер назначения ретрансляции, указанный для сопоставленного пула ретрансляции.

#### Пример

В этом примере показано, как настроить класс DHCP "Service-A", определенный с шаблоном соответствия DHCP Option 60 0x112233 и 0x102030, отнесенный к пулу ретрансляции "pool1" и связанный с целью ретрансляции "10.2.1.2".

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

## 15-2 ip dhcp class (DHCP Relay)

Эта команда используется для определения класса DHCP и входа в режим конфигурации класса DHCP. Для удаления класса DHCP используйте форму **no** этой команды.

```
ip dhcp class NAME
no ip dhcp class NAME
```

### Параметры

<i>NAME</i>	Указывает имя класса DHCP с максимальным количеством символов 32.
-------------	---

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте эту команду для входа в режим конфигурации класса DHCP. В этом режиме пользователь может использовать команду **option hex** для определения шаблона сопоставления опций для класса DHCP. Если класс не имеет связанной с ним опции option hex, класс будет соответствовать любому пакету.

### Пример

В этом примере показано, как настроить класс DHCP "Service-A" и определить его с помощью шаблона соответствия DHCP Option 60 0x112233.

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

## 15-3 ip dhcp pool (DHCP Relay)

Данная команда используется для настройки пула DHCP Relay на DHCP Relay Agent, а также для входа в режим настройки пула DHCP. Используйте форму **no**, чтобы удалить пул DHCP-Relay.

```
ip dhcp pool NAME
no ip dhcp pool NAME
```

### Параметры

<b>NAME</b>	Укажите имя пула адресов. Максимально допустимое количество символов – 32.
-------------	--

**По умолчанию**

Нет

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

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

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

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

**Пример**

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

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

**15-4 ip dhcp relay information check**

Данная команда позволяет включить в DHCP Relay Agent проверку/удаление информации Relay Agent Information Option (Option 82) в полученном пакете DHCP-ответа. Используйте форму **no** для общего отключения функции Check для Option 82.

**ip dhcp relay information check**  
**no ip dhcp relay information check**

**Параметры**

Нет

**По умолчанию**

По умолчанию данная функция отключена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Данная команда применима, если включен сервис DHCP.

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

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

Если функция Check отключена, пакет будет передан напрямую.

### Пример

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

```
Switch# configure terminal
Switch(config)# ip dhcp relay information check
Switch(config)#
```

## 15-5 ip dhcp relay information check-reply

Данная команда используется для настройки в DHCP Relay Agent проверки информации Relay Agent Information Option (Option 82) в полученном пакете DHCP-ответа. Используйте форму **no**, чтобы удалить данные настройки для интерфейса.

**ip dhcp relay information check-reply [none]**  
**no ip dhcp relay information check-reply**

### Параметры

<b>none</b>	(Опционально) Укажите, чтобы отключить функцию Check для Option 82 ответного пакета.
-------------	--

### По умолчанию

Нет

### Режим ввода команды

Interface Configuration Mode



## Использование команды

Данная команда применима, если включен сервис DHCP.

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

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

Если проверка отключена, пакет будет передан напрямую.

## Пример

В данном примере показано, как отключить общую функцию Check DHCP Relay Agent и включить функцию Check для VLAN 100. Включен рабочий режим функции Check для VLAN 100.

```
Switch# configure terminal
Switch(config)# no ip dhcp relay information check
Switch(config)# interface vlan 100
Switch(config-if)# ip dhcp relay information check-reply
Switch(config-if)#
```

## 15-6 ip dhcp relay information option

Данная команда используется для того, чтобы включить вставку информации о Relay Agent (Option 82) в ретранслируемых пакетах DHCP-запроса. Используйте форму **no**, чтобы отключить данную функцию.

**ip dhcp relay information option**  
**no ip dhcp relay information option**

### Параметры

Нет

### По умолчанию

По умолчанию Option 82 не встроена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Данная команда применима, если запущена команда **service dhcp**.

Если Option 82 DHCP запущена, в пакет DHCP, получаемый от клиента, будет встроено поле Option 82 перед ретрансляцией на сервер. Option 82 DHCP содержит две sub-опции: Circuit ID и Remote ID.

Команда **ip dhcp relay information option remote-id** используется для указания строки, задаваемой пользователем для sub-опции Remote ID.

### Пример

В данном примере показано, как встроить Option 82 в ретранслируемые пакеты DHCP-запроса.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)#
```

## 15-7 ip dhcp relay information option-insert

Данная команда используется для включения/выключения встраивания Option 82 для интерфейса в ретранслируемые пакеты DHCP-запроса. Используйте форму **no**, чтобы удалить настройки данной функции для интерфейса.

**ip dhcp relay information option-insert [none]**  
**no ip dhcp relay information option-insert**

### Параметры

<b>none</b>	(Опционально) Укажите, чтобы отключить встраивание Option 82 в ретранслируемый пакет.
-------------	---

### По умолчанию

Нет

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Данная команда применима, если запущена команда **service dhcp**.

### Пример

В данном примере показано, как включить функцию встраивания Option 82 в ретранслируемые пакеты DHCP-ответа и выключить данную функцию для интерфейса VLAN 100. Функция встраивания Option 82 выключена для VLAN 100, но включена для оставшихся интерфейсов.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# interface vlan 100
Switch(config-if)# ip dhcp relay information option-insert none
Switch(config-if)#
```

## 15-8 ip dhcp relay information policy

Данная команда используется для настройки алгоритма перенаправления Option 82 для DHCP Relay Agent. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip dhcp relay information policy {drop | keep | replace}
no ip dhcp relay information policy
```

### Параметры

<b>drop</b>	Укажите, чтобы отбросить пакет, у которого уже есть Relay Option.
<b>keep</b>	Укажите, чтобы напрямую в неизменном виде отправить пакет DHCP-запросов, у которого уже есть Relay Option, на DHCP-сервер.
<b>replace</b>	Укажите, чтобы заменить пакет DHCP-запросов, у которого уже есть Relay Option, новой опцией.

### По умолчанию

Параметр по умолчанию – **replace**.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Эта команда вступает в силу, когда включена команда **service dhcp**.

Используйте данную команду для настройки общего алгоритма встраивания Option 82 в пакеты, уже имеющие Option 82.

### Пример

В этом примере показано, как настроить политику повторной переадресации опций агента ретрансляции на сохранение.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information policy keep
Switch(config)#
```

## 15-9 ip dhcp relay information policy-action

Данная команда используется для настройки алгоритма перенаправления Option 82 для DHCP Relay Agent на интерфейсе. Используйте форму **no**, чтобы удалить настройки.

```
ip dhcp relay information policy-action {drop | keep | replace}
no ip dhcp relay information policy-action
```

### Параметры

<b>drop</b>	Укажите, чтобы отбросить пакет, у которого уже есть Relay Option.
<b>keep</b>	Укажите, чтобы в неизменном виде отправить пакет DHCP-запросов, у которого уже есть Relay Option, напрямую на DHCP-сервер.
<b>replace</b>	Укажите, чтобы заменить пакет DHCP-запросов, у которого уже есть Relay Option, новой опцией.

**По умолчанию**

Нет

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Данная команда применима, если запущен сервис DHCP. Используйте данную команду, чтобы настроить алгоритм встраивания Option 82 на интерфейсе в пакеты, у которых уже есть Option 82.

**Пример**

В данном примере показано, как настроить алгоритм перенаправления Relay Agent Option с помощью параметра keep, а также как настроить соответствующий алгоритм для VLAN 100 с помощью параметра drop. Для VLAN 100 эффективным алгоритмом перенаправления Relay Agent Option является drop, для других интерфейсов – keep.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information policy keep
Switch(config)# interface vlan 100
Switch(config-if)# ip dhcp relay information policy-action drop
Switch(config-if)#
```

**15-10 ip dhcp relay information option format remote-id**

Эта команда используется для настройки подварианта удаленного ID информации DHCP. Используйте форму по этой команды для настройки подпараметра удаленного ID по умолчанию.

**ip dhcp relay information option format remote-id {default | string SENTENCE | vendor2 | vendor3}**  
**no ip dhcp relay information option format remote-id**

**Параметры**

<b>default</b>	Укажите, чтобы использовать системный MAC-адрес коммутатора в качестве Remote ID. Формат Remote ID представлен ниже:
----------------	--

a.	b.	c.	d.	e.
2	8	0	6	MAC Address
1 byte	1 byte	1 byte	1 byte	6 bytes

**String SENTENCE**

Укажите, чтобы задать Remote ID самостоятельно.  
Допустимо использование пробелов. Формат Remote ID представлен ниже:

a.	b.	c.	d.	e.
2	n+2	1	n	User Defined
1 byte	1 byte	1 byte	1 byte	Max. 32 bytes

**vendor2**

Укажите, чтобы использовать vendor 2. Оригинальный формат Remote ID представлен ниже:

a.	b.	c.
2	n	System Name
1 byte	1 byte	n byte

**a. Tun sub-опции:** число 2 свидетельствует о том, что тип данного ID – Remote ID.

**b. Длина:** длина значения.

**c. Значение:** строка символов. Системное имя коммутатора.

**vendor3**

Указывает на использование производителя 3.

**По умолчанию**

В качестве строки удаленного идентификатора используется системный MAC-адрес коммутатора.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Данная команда используется для выбора различных vendor-ов или заданной пользователем строки ASCII в качестве Remote ID.

**Пример**

В данном примере показано, как настроить vendor2 в качестве Remote ID.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format remote-id vendor2
Switch(config)#
```

В данном примере показано, как настроить в качестве Remote ID строку, задаваемую пользователем. В примере используется строка «switch1».

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format remote-id string switch1
Switch(config)#
```

## 15-11 ip dhcp relay information option format-type remote-id

Эта команда используется для настройки подварианта удаленного ID информации DHCP в строке формата поставщика в режиме конфигурации интерфейса. Используйте форму **no** этой команды, чтобы удалить подвариант удаленного ID строки формата производителя.

```
ip dhcp relay information option format-type remote-id vendor3 string STRING
no ip dhcp relay information option format-type remote-id vendor3
```

### Параметры

<i>STRING</i>	Указывает пользовательскую строку.
<b>vendor3</b>	Указывает пользовательскую строку vendor 3 с максимальным количеством символов 32.

### По умолчанию

Нет

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Данная команда применима для настройки интерфейсов физического порта и интерфейсов port-channel. Используйте данную команду для настройки строки, определенной как vendor для sub-опции Remote ID Option 82 на интерфейсе.

### Пример

В этом примере показано, как определить строку формата vendor3 remote-id как "switch1" на порту 3.

```
Switch# configure terminal
Switch(config)# interface eth1/0/3
Switch(config-if)# ip dhcp relay information option format-type remote-id vendor3
string switch1
Switch(config-if)#
```

## 15-12 ip dhcp relay information option format circuit-id

Эта команда используется для настройки подварианта ID схемы информации DHCP. Используйте форму **no** этой команды для настройки подпараметра ID схемы по умолчанию.

```
ip dhcp relay information option format circuit-id {default | string SENTENCE | vendor1 | vendor2|
vendor3| vendor4 | vendor5 | vendor6}
no ip dhcp relay information option format circuit-id
```

## Параметры

### default

Укажите, чтобы использовать sub-опцию Circuit ID по умолчанию. Оригинальный формат Circuit ID представлен ниже:

```
-----|
| a.   | b.   | c.   | d.   | e.   | f.   | g.   |
|-----|
| 1    | 0x6  | 0    | 4    | VLAN | Module | Port |
|      |      |      |      |      | ID     | ID   |
|-----|
| 1 byte | 1 byte | 1 byte | 1 byte | 2 bytes | 1 byte | 1 byte |
|-----|
```

- a. *Tun sub-опции*: число 1 свидетельствует о том, что типданного ID – Circuit ID.
- b. *Длина*: длина значения. Необходимая длина значения – 6.
- c. *Sub-опция Circuit ID*: необходимое значение – 0.
- d. *Длина sub-опции*: необходимое значение – 4.
- e. *VLAN ID (S-VID)*.
- f. *ID модуля*: необходимое значение для автономных коммутаторов – 0.
- g. *ID порта*: номер порта для каждого Unit ID.

### SENTENCE

Укажите, чтобы задать Circuit ID самостоятельно. Допустимо использование пробелов.

```
-----|
| a.   | b.   | c.   | d.   | e.   |
|-----|
| 2    | n+2  | 1    | n    | User Defined |
|-----|
| 1 byte | 1 byte | 1 byte | 1 byte | Max. 32 bytes |
|-----|
```

### vendor1

Укажите, чтобы использовать vendor1. Формат Circuit ID представлен ниже:

a.	b.	c.	d.	e.	f.
1	0x10	0	6	VLAN	Slot ID
1 byte	1 byte	1 byte	1 byte	2 bytes	2 bytes

  

g.	h.	i.	j.
Port ID	1	6	MAC
2 bytes	1 byte	1 byte	6 bytes

- a.** *Tun sub-опции:* число 1 свидетельствует о том, что типданного ID – Circuit ID.
- b.** *Длина.*
- c.** *Первый тег sub-опции Circuit ID:* необходимое значение – 0.
- d.** *Длина первого тега:* необходимое значение – 6.
- e.** *VLAN ID.*
- f.** *ID слота:* необходимое значение для автономных коммутаторов – 1, для стекируемых коммутаторов – Unit ID встеке.
- g.** *ID порта:* номер порта для каждого Unit ID.
- h.** *Второй тег sub-опции Circuit ID:* необходимозначение – 1.
- i.** *Длина второго тега:* необходимое значение – 6.
- j.** *MAC-адрес:* системный MAC-адрес коммутатора.

<b>vendor2</b>	Указывает использовать vender2.
<b>vendor3</b>	Указывает использовать vender3.
<b>vendor4</b>	Указывает использовать vender4.
<b>vendor5</b>	Указывает использовать vender5.
<b>vendor6</b>	Указывает использовать vender6.

#### По умолчанию

Формат идентификатора цепи: идентификатор VLAN, номер модуля и номер порта.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Данная команда используется для выбора различных vendor-ов или заданной пользователем строки ASCII в качестве Circuit ID.

#### Пример

В данном примере показано, как использовать vendor1 в качестве Circuit ID.



```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format circuit-id vendor1
Switch(config)#
```

В данном примере показано, как настроить в качестве Circuit ID строку, задаваемую пользователем. В примере используется строка «abcd».

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format circuit-id string abcd
Switch(config)#
```

### 15- 13 ip dhcp relay information option format-type circuit-id

Эта команда используется для настройки подварианта ID информационной схемы DHCP в строке, определяемой пользователем.

```
ip dhcp relay information option format-type circuit-id vendor3 string STRING
no ip dhcp relay information option format-type circuit-id vendor3 string
```

#### Параметры

<i>STRING</i>	Указывает строку, определяемую поставщиком.
<b>vendor3</b>	Указывает на пользовательскую строку vendor3, содержащую не более 32 символов.

#### По умолчанию

Нет

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и интерфейсов port-channel. Используйте данную команду для настройки строки, определенной как vendor для sub-опции Circuit ID Option 82 на интерфейсе.

#### Пример

В этом примере показано, как определить vendor3 circuit-id "abc" на порту 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ip dhcp relay information option format-type circuit-id vendor3
string abc
Switch(config-if)#
```

## 15-14 ip dhcp relay information trust-all

Данная команда позволяет назначить на DHCP Relay Agent все интерфейсы, отправляющие информацию об IP DHCP Relay, доверенными. Используйте форму **no**, чтобы отключить функцию Trust для всех интерфейсов.

```
ip dhcp relay information trust-all
no ip dhcp relay information trust-all
```

### Параметры

Нет

### По умолчанию

По умолчанию данная функция отключена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Если на интерфейсе включена опция Trust для информации IP DHCP Relay, будут приниматься пакеты, GIADDR которых равен 0 (данный Relay Agent является первой ретрансляцией данного пакета DHCP-запроса), но у которых присутствует Relay Agent Information Option (Option 82). Если интерфейс не является доверенным, пакеты будут отброшены.

Если применены настройки данной команды, информация IP DHCP Relay является доверенной со всех интерфейсов. Если настройки данной команды не применены, статус информации определяется командой **ip dhcp relay information trusted** в режиме интерфейса.

Проверить настройки можно при помощи команды **show ip dhcp relay information trusted-sources**.

### Пример

В данном примере показано, как назначить на DHCP Relay Agent информацию IP DHCP Relay в качестве доверенной со всех интерфейсов. Информация Relay считается доверенной со всехинтерфейсов, вне зависимости от настроек команды **ip dhcp relay information trusted**.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information trust-all
Switch(config)#
```

## 15-15 ip dhcp relay information trusted

Данная команда позволяет назначить на DHCP Relay Agent определенный интерфейс, отправляющий информацию об IP DHCP Relay, в качестве доверенного. Используйте форму **no**, чтобы отключить функцию Trust для интерфейса.

```
ip dhcp relay information trusted
no ip dhcp relay information trusted
```

**Параметры**

Нет

**По умолчанию**

По умолчанию информация не является доверенной.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Если информация IP DHCP Relay отправляется с доверенного интерфейса, будут приниматься пакеты, GIADDR которых равен 0 (данный Relay Agent является первой ретрансляцией данного пакета DHCP-запроса), но у которых присутствует Relay Agent Information Option (Option 82). Если интерфейс не является доверенным, пакеты будут отброшены.

Если применены настройки команды `trust-all`, информация IP DHCP Relay является доверенной со всех интерфейсов. Если настройки данной команды не применены, статус информации определяется командой `ip dhcp relay information trusted` в режиме интерфейса.

Проверить настройки можно при помощи команды `show ip dhcp relay information trusted-sources`.

**Пример**

В данном примере показано, как на DHCP Relay Agent снять статус Trust для всех интерфейсов и запустить статус Trust для VLAN 100.

```
Switch# configure terminal
Switch(config)# no ip dhcp relay information trust-all
Switch(config)# interface vlan 100
Switch(config-if)# ip dhcp relay information trusted
Switch(config-if)#
```

**15- 16 ip dhcp local-relay vlan**

Данная команда используется для включения Local Relay на одной из VLAN или группе VLAN. Используйте форму `no`, чтобы отключить данную функцию.

```
ip dhcp local-relay vlan VLAN-ID [, | -]
no ip dhcp local-relay vlan VLAN-ID [, | -]
```

**Параметры**

<code>VLAN-ID</code>	Укажите используемую VLAN.
<code>,</code>	(Опционально) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
<code>-</code>	(Опционально) Используется для обозначения диапазона

---

**VLAN. Пробелы до и после дефиса недопустимы.**

---

**По умолчанию**

По умолчанию данная функция отключена.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Local Relay обеспечивает передачу сообщения DHCP на все локальные порты-участники VLAN на основе настроек Relay Option. Local Relay не изменяет IP-адрес и MAC-адрес назначения, а также поле шлюза пакета.

**Пример**

В данном примере показано, как включить функцию Local Relay на VLAN 100.

```
Switch# configure terminal
Switch(config)# ip dhcp local-relay vlan 100
Switch(config)#
```

**15-17 ip dhcp smart-relay**

Эта команда используется для включения функции интеллектуальной ретрансляции агента ретрансляции DHCP. Используйте форму **no** этой команды для отключения функции интеллектуальной эстафеты.

```
ip dhcp smart-relay
no ip dhcp smart-relay
```

**Параметры**

Нет

**По умолчанию**

По умолчанию эта опция отключена

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Если полученный интерфейс пакета имеет вторичные адреса, по умолчанию агент ретрансляции устанавливает в поле адреса шлюза пакета первичный адрес интерфейса. Если включена интеллектуальная ретрансляция, агент ретрансляции будет подсчитывать количество повторных попыток отправки клиентом сообщения DISCOVER. После трех повторных попыток агент ретрансляции изменит адрес шлюза на вторичный адрес полученного интерфейса.

**Пример**

В этом примере показано, как включить функцию интеллектуального реле.

```
Switch# configure terminal
Switch(config)# ip dhcp smart-relay
Switch(config)#
```

## 15-18 option hex (DHCP Relay)

Эта команда используется для указания шаблона соответствия опций DHCP для класса DHCP. Используйте форму **no** этой команды для удаления указанного шаблона соответствия для класса DHCP.

**option** *CODE* **hex** *PATTERN* [\*] [**bitmask** *MASK*]  
**no option** *CODE* **hex** *PATTERN* [\*] [**bitmask** *MASK*]

### Параметры

<i>CODE</i>	Указывает номер опции DHCP.
<i>PATTERN</i>	Указывает шестнадцатеричный шаблон указанного параметра DHCP.
*	(Опционально) Указывает не сопоставлять оставшиеся биты параметра. Если не указано, длина бита <i>PATTERN</i> должна быть равна такой же, как длина бита опции.
<i>MASK</i>	(Опционально) Указывает шестнадцатеричную битовую маску для маскирования шаблона. Будут проверяться маскированные биты шаблона. Если не указано, будут проверены все биты, указанные в <i>PATTERN</i> . Бит, установленный в FF, будет проверен. Формат ввода должен быть таким же, как и у <i>PATTERN</i> .

### По умолчанию

Нет

### Режим ввода команды

DHCP Class Configuration Mode.

### Использование команды

Используйте команду **ip dhcp class** вместе с этой командой для определения класса DHCP. Классы в пуле сопоставляются в последовательности конфигурации классов в пуле.

С помощью команды **option hex** пользователь может указать номер кода опции DHCP с его шаблоном сопоставления для класса DHCP. Для класса DHCP можно указать несколько шаблонов опций. Если пакет соответствует любому из указанных шаблонов класса DHCP, пакет будет отнесен к классу DHCP и перенаправлен в соответствии с указанной целью.

Ниже перечислены некоторые часто используемые коды опций:

- Option 60: идентификатор класса поставщика.
- Option 61: идентификатор клиента.
- Option 77: класс пользователя.
- Option 124: класс поставщика, идентифицирующий поставщика.

- Option 125: информация, идентифицирующая конкретного поставщика.

### Пример

В этом примере показано, как настроить класс DHCP "Service-A" для определения с помощью DHCP Option 60 шаблона соответствия 0x112233 и 0x102030.

```
Switch# configure terminal
Switch(config)# ip dhcp class Service-A
Switch(config-dhcp-class)# option 60 hex 112233
Switch(config-dhcp-class)# option 60 hex 102030
Switch(config-dhcp-class)#
```

## 15-19 relay destination

Данная команда используется для указания IP-адреса DHCP Relay Destination, ассоциированного с Relay-пулом. Используйте форму **no**, чтобы удалить Relay Destination из пула DHCP-Relay.

**relay destination** *IP-ADDRESS*  
**no relay destination** *IP-ADDRESS*

### Параметры

<i>IP-ADDRESS</i>	Укажите IP-адрес DHCP Relay Destination Server.
-------------------	---

### По умолчанию

Нет

### Режим ввода команды

DHCP Pool Configuration Mode

### Использование команды

Наряду с пакетами DHCP Relay, подчиняющимися команде **ip helper-address**, Relay Destination DHCP-сервера можно указать в пуле DHCP Relay. Для этого войдите в режим настройки пула DHCP при помощи команды **ip dhcp pool**, затем при помощи команды **relay source** укажите подсеть-источник (source) запросов клиента, после чего при помощи команды **relay destination** укажите адрес Relay Destination Server. В пуле можно указать несколько Relay Sources и несколько Relay Destinations. Если пакет соответствует какому-либо из Relay Sources, он будет отправлен на все Relay Destinations.

Если подсеть, от которой приходит пакет DHCP-запроса, соответствует Relay Source Relay-пула, пакет будет ретранслирован на основе данного пула. В других случаях пакет ретранслируется на основе IP Helper-адреса, настроенного для получающего интерфейса. Чтобы ретранслировать пакет на основе пула DHCP Relay, если пакет запроса является ретранслируемым пакетом, источником запроса должен быть GIADDR (IP-адрес шлюза) пакета. Если пакет запроса не является ретранслируемым пакетом, источником пакета является подсеть получающего интерфейса.

В пуле DHCP Relay администратор может далее использовать команды **class** и **relay target**, чтобы связать список адресов Relay Target с классом DHCP.

## Пример

В данном примере показано, как создать пул DHCP Relay под именем «pool1». В Relay-пуле подсеть 172.19.10.0/255.255.255.0 указана в качестве подсети-источника (source), а 10.2.1.1 указан в качестве адреса Relay Destination.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# relay source 172.19.10.0 255.255.255.0
Switch(config-dhcp-pool)# relay destination 10.2.1.1
Switch(config-dhcp-pool)#
```

## 15-20 relay source

Данная команда используется для указания подсети-источника (source) пакетов клиента. Используйте форму **no**, чтобы удалить подсеть-источник (source).

**relay source** IP-ADDRESS SUBNET-MASK  
**no relay source** IP-ADDRESS SUBNET-MASK

### Параметры

<i>IP-ADDRESS</i>	Укажите исходную подсеть-источник (source) пакетов клиента.
<i>SUBNET-MASK</i>	Укажите маску подсети-источника (source).

### По умолчанию

Нет

### Режим ввода команды

DHCP Pool Configuration Mode

### Использование команды

Наряду с пакетами DHCP Relay, подчиняющимися команде **ip helper-address**, Relay Destination DHCP-Relay-сервера можно указать в пуле DHCP Relay. Для этого войдите в режим настройки пула DHCP при помощи команды **ip dhcp pool**, затем при помощи команды **relay source** укажите подсеть-источник (source) запросов клиента, после чего при помощи команды **relay destination** укажите адрес Relay Destination Server. В пуле можно указать несколько Relay Sources и несколько Relay Destinations. Если пакет соответствует какому-либо из Relay Sources, он будет отправлен на все Relay Destinations.

При получении пакета DHCP-запроса, если подсеть полученного пакета соответствует Relay Source

Relay-пула, пакет будет ретранслирован на основе данного пула. В других случаях пакет ретранслируется на основе IP Helper-адреса, настроенного для получающего интерфейса. Чтобы ретранслировать пакет на основе пула DHCP Relay, если пакет запроса является ретранслируемым пакетом, источником запроса должен быть GIADDR (IP-адрес шлюза) пакета. Если пакет запроса не является ретранслируемым пакетом, подсеть получающего интерфейса является источником пакета.

В пуле DHCP Relay администратор может далее использовать команды **class** и **relay target**, чтобы связать список адресов Relay Target с классом DHCP. DHCP-пакет не будет ретранслирован, если на интерфейсе, принимающем пакет, не настроен IP-адрес.

### Пример

В данном примере показано, как создать пул DHCP Relay «pool2». В Relay-пуле подсеть 172.19.18.0/255.255.255.0 указана в качестве подсети-источника (source), а 10.2.1.10 указан в качестве адреса Relay Destination.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool2
Switch(config-dhcp-pool)# relay source 172.19.18.0 255.255.255.0
Switch(config-dhcp-pool)# relay destination 10.2.1.10
Switch(config-dhcp-pool)#
```

## 15-21 relay target

Данная команда используется для указания DHCP Relay Target для ретранслируемых пакетов, которая соответствует шаблону значений опции, установленной в классе. Используйте форму **no**, чтобы удалить Relay Target.

**relay target** IP-ADDRESS  
**no relay target** IP-ADDRESS

### Параметры

IP-ADDRESS	Укажите IP-адрес сервера Relay Target для класса.
------------	---

### По умолчанию

Нет

### Режим ввода команды

DHCP Pool Class Configuration Mode

### Использование команды

В пуле DHCP Relay администратор может далее использовать команды **class** и **relay target**, чтобы связать список адресов Relay Target с классом DHCP. Если запрос клиента соответствует Relay-пулу, а пул DHCP Relay настроен с классами, для ретрансляции запрос клиента должен соответствовать классу, указанному в пуле. Если пакет не соответствует ни одному из классов пула, он не будет повторно ретранслирован. Если класс соответствующего Relay-пула не определен, запрос будет ретранслирован в Relay Destination соответствующего Relay-пула. Для класса можно указать несколько команд Relay Target. Если пакет соответствует классу, он будет направлен во все Relay Targets (Destination).

Если для класса не настроена команда **relay target**, за Relay Target будет принято Relay Destination, указанное для пула. DHCP-пакет не будет ретранслирован, если на интерфейсе, принимающем пакет, не настроен IP-адрес.

### Пример



В данном примере показано, как настроить DHCP Relay Target для ретрансляции пакетов, которая соответствует образцу значений опции, установленной в классе.

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

## 15-22 service dhcp (DHCP Relay)

Эта команда используется для включения службы ретрансляции DHCP на коммутаторе. Используйте форму **no** этой команды для отключения службы ретрансляции DHCP.

**service dhcp**  
**no service dhcp**

### Параметры

Нет

### По умолчанию

По умолчанию эта опция отключена

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте эту команду для включения или отключения службы ретрансляции DHCP на коммутаторе.

### Пример

В этом примере показано, как отключить службу ретрансляции DHCP.

```
Switch#configure terminal
Switch(config)#no service dhcp
Switch(config)#
```

## 15-23 show ip dhcp relay information trusted-sources

Данная команда используется для отображения всех интерфейсов, настроенных в качестве доверенных источников для опции DHCP Relay.

**show ip dhcp relay information trusted-sources**

### Параметры

Нет

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте данную команду для отображения рабочих настроек функции Trust Relay Option.

### Пример

В этом примере показано, как отобразить эффективную настройку функции опции trust relay information, когда команда **ip dhcp relay information trust-all** отключена.

```
Switch# show ip dhcp relay information trusted-sources

List of trusted sources of relay agent information option:
vlan 100          vlan 200          vlan 300          vlan 400
vlan 500

Total Entries: 5

Switch#
```

В этом примере показано, как отобразить эффективную настройку функции опции trust relay information, когда команда **ip dhcp relay information trust-all** включена.

```
Switch# show ip dhcp relay information trusted-sources

All interfaces are trusted source of relay agent information option

Switch#
```

## 15-24 show ip dhcp relay information option-insert

Эта команда используется для отображения конфигурации вставки опции relay.

### show ip dhcp relay information option-insert

### Параметры

Нет

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте данную команду для отображения Relay Information Option и информации о настройке встраивания.

### Пример

В данном примере показано, как отобразить информацию об Option 82 и информацию о настройке встраивания этой опции для всех VLAN.

```
Switch# show ip dhcp relay information option-insert

Interface      Option-Insert
-----
vlan1          Enabled
vlan2          Disabled
vlan3          Not Configured

Total Entries: 3

Switch#
```

## 15-25 show ip dhcp relay information policy-action

Данная команда используется для отображения информации об алгоритме перенаправления Relay Option для интерфейса.

**show ip dhcp relay information policy-action**

### Параметры

Нет

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте эту команду для отображения информации о конфигурации действий политики опции relay information.

### Пример

В данном примере показано, как отобразить информацию об алгоритме перенаправления Option 82 для всех VLAN.

```
Switch# show ip dhcp relay information policy-action
```

Interface	Policy
-----	-----
vlan1	Keep
vlan2	Drop
vlan3	Replace
vlan4	Not configured

```
Total Entries: 4
```

```
Switch#
```

## 16. Команды DHCP Snooping

### 16-1 ip dhcp snooping

Данная команда используется для глобального включения DHCP Snooping. Используйте форму **no**, чтобы отключить DHCP Snooping.

```
ip dhcp snooping
no ip dhcp snooping
```

#### Параметры

Нет

#### По умолчанию

По умолчанию опция отключена.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Функция DHCP Snooping отслеживает пакеты DHCP, поступающие на недоверенный интерфейс во VLAN, на котором включена данная функция. С помощью данной функции DHCP-пакеты, приходящие с недоверенного интерфейса, могут получить статус проверенных и будет создана таблица привязки DHCP для DHCP Snooping во VLAN. Таблица привязки содержит информацию о привязке IP и MAC, которая позже дополнительно может использоваться IP Source Guard и Dynamic ARP Inspection.

#### Пример

В данном примере показано, как включить DHCP Snooping.

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

### 16-2 ip dhcp snooping information option allow-untrusted

Данная команда используется для глобального доступа DHCP-пакетов с Relay Option 82 к недоверенным интерфейсам. Используйте форму **no**, чтобы запретить пакеты с Relay Option 82.

```
ip dhcp snooping information option allow-untrusted
no ip dhcp snooping information option allow-untrusted
```

#### Параметры

Нет

#### По умолчанию

По умолчанию опция отключена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Функция DHCP Snooping проверяет пакеты DHCP, когда они поступают на порт во VLAN, на котором включена функция DHCP Snooping. По умолчанию при проверке будут отброшены пакеты, если их адрес шлюза не равен 0 или присутствует Option 82.

Используйте данную команду, чтобы разрешить пакетам с Relay Option 82 доступ к недоверенным интерфейсам.

### Пример

В данном примере показано, как включить DHCP Snooping для Option 82, чтобы разрешить доступ к недоверенным интерфейсам.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping information option allow-untrusted
Switch(config)#
```

## 16-3 ip dhcp snooping database

Данная команда используется для настройки хранения записей привязки DHCP Snooping в локальной файловой системе (флеш-карте) или на удаленном узле. При использовании формы **no** команда отключит хранение или вернется к настройкам по умолчанию.

```
ip dhcp snooping database {URL /write-delay SECONDS}
no ip dhcp snooping database [write-delay]
```

### Параметры

<i>URL</i>	Укажите URL в каком-либо из представленных форматов: <ul style="list-style-type: none"> <li>tftp://location/filename</li> </ul>
<b>write-delay SECONDS</b>	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

### Использование команды

Данная команда используется для хранения записей привязки DHCP в локальной Flash-памяти или на удаленном узле. Используйте следующие методы для хранения записей привязки DHCP:

- **tftp**: хранение записей на удаленном узле через TFTP.

Используйте данную команду, чтобы сохранить таблицу привязки DHCP Snooping в коммутаторе стека. Таблица не будет сохранена в отдельных коммутаторах стека.

Время аренды записи (Lease Time) не будет изменено, и время жизни (Live Time) продолжит отсчитываться, пока запись существует.

### Пример

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

```
Switch# configure terminal
Switch(config)# ip dhcp snooping database tftp: //10.0.0.2/store/dhcp-snp-bind
Switch(config)#
```

## 16-4 clear ip dhcp snooping database statistics

Данная команда используется для удаления статистики таблицы привязки DHCP.

**clear ip dhcp snooping database statistics**

### Параметры

Нет

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Данная команда позволяет удалить статистику таблицы привязки DHCP.

### Пример

В данном примере показано, как удалить статистику таблицы привязки DHCP Snooping.

```
Switch# clear ip dhcp snooping database statistics
Switch#
```

## 16-5 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**

<i>MAC-ADDRESS</i>	(Опционально) Укажите MAC-адрес, который необходимо удалить.
<i>IP-ADDRESS</i>	(Опционально) Укажите IP-адрес, который необходимо удалить.
<b>vlan</b> <i>VLAN-ID</i>	(Опционально) Укажите VLAN ID, который необходимо удалить.
<b>interface</b> <i>INTERFACE-ID</i>	(Опционально) Укажите интерфейс, который необходимо удалить.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Данная команда позволяет удалить запись привязки DHCP, включая заданные вручную записи привязки.

**Пример**

В данном примере показано, как удалить все записи привязки DHCP Snooping.

```
Switch# clear ip dhcp snooping binding
Switch#
```

**16-6 renew ip dhcp snooping database**

Данная команда используется для обновления таблицы привязки DHCP.

**renew ip dhcp snooping database** *URL*

**Параметры**

<i>URL</i>	URL может быть в одном из следующих форматов: <ul style="list-style-type: none"> <li>tftp://location/filename</li> </ul>
------------	--

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**



Используйте эту команду для загрузки базы данных записей привязки из URL и добавления записей в таблицу записей привязки DHCP snooping.

### Пример

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

```
Switch# renew ip dhcp snooping database tftp: //10.0.0.2/store/dhcp-snp-bind
Switch#
```

## 16-7 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

<i>MAC-ADDRESS</i>	Укажите MAC-адрес записи, которую необходимо добавить или удалить.
<b>vlan</b> <i>VLAN-ID</i>	Укажите VLAN ID записи, которую необходимо добавить или удалить.
<i>IP-ADDRESS</i>	Укажите IP-адрес записи, которую необходимо добавить или удалить.
<i>INTERFACE-ID</i>	Укажите интерфейс (физический порт или port-channel), на котором необходимо добавить или удалить запись привязки.
<i>SECONDS</i>	Укажите интервал, после которого привязки не будут действительны. Доступен диапазон значений от 60 до 4294967295 секунд.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Эта команда доступна только для конфигурации физического порта и интерфейса порт-канала. Используйте эту команду для создания динамической записи DHCP snooping.

### Пример

В данном примере показано, как настроить запись DHCP Snooping с IP-адресом 10.1.1.1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 и порту Ethernet 1/0/10 с expiry time 100 секунд.

```
Switch# ip dhcp snooping binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface eth1/0/10 expiry
100
Switch#
```

## 16-8 ip dhcp snooping trust

Данная команда используется для настройки порта в качестве доверенного интерфейса для DHCP Snooping. При использовании формы **no** команда вернется к значениям по умолчанию.

```
ip dhcp snooping trust
no ip dhcp snooping trust
```

### Параметры

Нет

### По умолчанию

По умолчанию данная опция отключена.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Данная команда позволяет настроить физический порт и port-channel интерфейс.

Порты, подключенные к DHCP-серверу или к другим коммутаторам, должны быть настроены как доверенные интерфейсы. Порты, подключенные к DHCP-клиентам, должны быть настроены как недоверенные интерфейсы. DHCP Snooping работает в качестве межсетевого экрана между недоверенными интерфейсами и DHCP-серверами.

Если порт настроен как недоверенный интерфейс, сообщение DHCP придет на порт в ту VLAN, в которой включен DHCP Snooping. Коммутатор перенаправит пакеты DHCP, если только не будет соблюдаться любое из следующих условий (в таком случае пакеты будут отбрасываться):

- Порт коммутатора получает пакет (например, пакет DHCP OFFER, DHCP ACK, DHCP NAK или DHCP REQUEST) от DHCP-сервера за пределами межсетевого экрана.
- Если включена команда **ip dhcp snooping verify mac-address**, чтобы пройти проверку, MAC-адрес источника в заголовке Ethernet должен быть таким же, как и аппаратный адрес DHCP-клиента.
- Недоверенный интерфейс получает DHCP-пакет, включающий в себя IP-адрес агента ретрансляции (Relay Agent), отличный от 0.0.0.0, или Relay Agent перенаправляет пакет, включающий в себя Option 82 на недоверенный интерфейс.
- Маршрутизатор получает сообщение DHCP RELEASE или DHCP DECLINE 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 этом примере показано, как включить доверие DHCP snooping для порта 3.

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

## 16-9 ip dhcp snooping limit entries

Данная команда используется для настройки количества записей привязки DHCP Snooping, которые может изучить интерфейс. При использовании формы **no** команда сбросит значение лимита записей DHCP.

```
ip dhcp snooping limit entries {NUMBER}
no ip dhcp snooping limit entries
```

### Параметры

<i>NUMBER</i>	Укажите лимит количества привязок DHCP Snooping на порт. Диапазон допустимых значений: от 0 до 1024.
---------------	--

### По умолчанию

По умолчанию этот параметр имеет значение **no-limit**.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Данная команда позволяет настроить физический порт и интерфейс port-channel. Команда действует только на недоверенных интерфейсах. Система перестанет изучать привязки, связанные с портом, если превышено максимальное значение.

### Пример

В этом примере показано, как настроить ограничение на количество записей привязки, разрешенных на порту 1 до 100.

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

## 16-10 ip dhcp snooping limit rate

Данная команда используется для настройки количества DHCP-сообщений, которые интерфейс сможет получать за секунду. При использовании формы **no** команда сбросит значение лимита сообщений DHCP.

```
ip dhcp snooping limit rate {VALUE}
no ip dhcp snooping limit rate
```

### Параметры

---

<i>VALUE</i>	Укажите количество DHCP-сообщений, которое может быть обработано за секунду. Диапазон допустимых значений: от 1 до 300.
--------------	---

---

### По умолчанию

По умолчанию этот параметр отключен.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Если скорость передачи DHCP-пакета превышает установленное ограничение, порт переходит в состояние error disable.

### Пример

В этом примере показано, как настроить количество сообщений DHCP, которые коммутатор может принимать в секунду на порту 3.

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

## 16-11 ip dhcp snooping station-move deny

Данная команда используется для отключения состояния DHCP Snooping Station Move. При использовании формы **no** команда включит состояние DHCP Snooping Roaming.

**ip dhcp snooping station-move deny**  
**no ip dhcp snooping station-move deny**

### Параметры

Нет

### По умолчанию

По умолчанию опция включена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

При включении DHCP Snooping Station Move динамическая запись привязки DHCP Snooping с теми же VLAN ID и MAC-адресом на определенном порту может переместиться на другой порт, если обнаружится, что новому процессу DHCP принадлежит тот же VLAN ID и MAC-адрес.

### Пример

В данном примере показано, как отключить состояние Roaming.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping station-move deny
Switch(config)#
```

## 16-12 ip dhcp snooping verify mac-address

Данная команда используется для включения проверки совпадения MAC-адреса источника DHCP-пакета и аппаратного адреса клиента. При использовании формы **no** команда отключит проверку MAC-адреса.

```
ip dhcp snooping verify mac-address
no ip dhcp snooping verify mac-address
```

### Параметры

Нет

### По умолчанию

По умолчанию опция включена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

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

### Пример

В данном примере показано, как включить проверку на соответствие MAC-адреса источника DHCP-пакета аппаратному адресу клиента.

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

## 16-13 ip dhcp snooping vlan

Данная команда используется для включения DHCP Snooping во VLAN или группе VLAN. При использовании формы **no** команда отключит DHCP Snooping во VLAN или группе VLAN.

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

### Параметры

<i>VLAN-ID</i>	Указание используемой сети VLAN.
,	(Опционально) Выделение серии VLAN или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Выделение диапазона VLAN. Пробелы до и после дефиса недопустимы.

### По умолчанию

По умолчанию функция DHCP Snooping отключена во всех VLAN.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду для глобального включения DHCP Snooping, используйте команду **ip dhcp snooping vlan** для включения DHCP Snooping для VLAN. Функция DHCP Snooping отслеживает пакеты DHCP, приходящие на недоверенный интерфейс во VLAN, на которой включена функция DHCP snooping. С помощью данной функции DHCP-пакеты, приходящие с недоверенного интерфейса, могут получить статус проверенных, а таблица привязки DHCP будет создана для DHCP Snooping во VLAN. Таблица привязки предоставляет информацию о привязке IP и MAC, которая позже может использоваться IP Source Guard и Dynamic ARP Inspection.

### Пример

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

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

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

```
Switch# configure terminal
Switch(config)# ip dhcp snooping vlan 10,15-18
Switch(config)#
```

## 16- 14 show ip dhcp snooping

Данная команда используется для отображения настроек DHCP Snooping.

**show ip dhcp snooping**

### Параметры

Нет

### По умолчанию

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Данная команда используется для отображения параметров настроек DHCP Snooping.

**Пример**

В данном примере показано, как включить отображение параметров настроек DHCP Snooping.

```
Switch# show ip dhcp snooping

DHCP Snooping is disabled
DHCP Snooping is enabled on VLANs:
    1-4094
Verification of MAC address is enabled
Station move is permitted.
Information option is not allowed on un-trusted interface

Interface      Trusted   Rate Limit   Entry Limit
-----
eth1/0/1       no       10           no_limit
eth1/0/2       no       no_limit     no_limit
eth1/0/3       no       no_limit     no_limit
eth1/0/4       no       no_limit     no_limit
eth1/0/5       no       no_limit     no_limit
eth1/0/6       no       no_limit     no_limit
eth1/0/7       no       no_limit     no_limit
eth1/0/8       no       50           20
eth1/0/9       yes      no_limit     no_limit
eth1/0/10      no       no_limit     no_limit
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

**16-15 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]
[l,|-l]
```

**Параметры**

<i>IP-ADDRESS</i>	(Опционально) Укажите, если необходимо отображать привязки на основе IP-адреса.
<i>MAC-ADDRESS</i>	(Опционально) Укажите, если необходимо отображать

	привязки на основе MAC-адреса.
<b>vlan</b> <i>VLAN-ID</i>	(Опционально) Укажите, если необходимо отображать привязки на основе VLAN.
<b>interface</b> <i>INTERFACE-ID</i>	(Опционально) Укажите, если необходимо отображать привязки на основе ID порта (port ID).
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Выделение диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Данная команда используется для отображения привязки DHCP Snooping.

**Пример**

В данном примере показано, как настроить отображение привязки DHCP Snooping.

```
Switch#show ip dhcp snooping binding
```

```

MAC Address      IP Address      Lease (seconds) Type          VLAN Interface
-----
00-01-02-03-04-05 10.1.1.10      1500          dhcp-snooping 100 eth1/0/5
00-01-02-00-00-05 10.1.1.11      1495          dhcp-snooping 100 eth1/0/5

Total Entries: 2

Switch#
```

В данном примере показано, как настроить отображение привязки DHCP Snooping по IP 10.1.1.1.

```
Switch# show ip dhcp snooping binding 10.1.1.1
```

```

MAC Address      IP Address      Lease (seconds) Type          VLAN Interface
-----
00-01-02-03-04-05 10.1.1.1      1500          dhcp-snooping 100 eth1/0/5

Total Entries: 1

Switch#
```

В данном примере показано, как настроить отображение привязки DHCP Snooping по IP 10.1.1.11 и MAC 00-01-02-00-00-05.



```
Switch# show ip dhcp snooping binding 10.1.1.11 00-01-02-00-00-05

MAC Address      IP Address      Lease(seconds)  Type           VLAN Interface
-----
00-01-02-00-00-05 10.1.1.11      1495            dhcp-snooping 100 eth1/0/5

Total Entries: 1

Switch#
```

В данном примере показано, как настроить отображение привязки DHCP Snooping по IP 10.1.1.1 и MAC 00-01-02-03-04-05 во VLAN 100.

```
Switch# show ip dhcp snooping binding 10.1.1.11 00-01-02-00-00-05 vlan 100

MAC Address      IP Address      Lease(seconds)  Type           VLAN Interface
-----
00-01-02-03-04-05 10.1.1.11      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

<b>MAC-адрес</b>	Аппаратный MAC-адрес клиента.
<b>IP-адрес</b>	IP-адрес клиента, назначенный DHCP-сервером.
<b>Время аренды (lease) (в секундах)</b>	Время аренды IP-адреса.

<b>Тип</b>	Тип привязки, настроенный через интерфейс командной строки или изученный динамически.
<b>VLAN</b>	VLAN ID.
<b>Interface</b>	Интерфейс, подключающийся к узлу DHCP-клиента.

## 16-16 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

EXEC Mode

#### 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

<b>Binding Collisions</b>	Количество записей, создавших коллизии с существующими записями в таблице привязки DHCP Snooping.
<b>Expired leases</b>	Количество записей с истекшим сроком аренды в таблице привязки DHCP Snooping.
<b>Invalid interfaces</b>	Количество интерфейсов, получивших сообщение DHCP, но DHCP Snooping для которых не выполняется.
<b>Pase failures</b>	Количество недопустимых пакетов DHCP.

<b>Checksum errors</b>	Количество подсчитанных значений checksum, не равное сохраненному значению checksum.
<b>Unsupported vlans</b>	Количество записей, для которых VLAN отключена.

## 16-17 based-on hardware-address

Эта команда используется для добавления записи профиля экрана сервера DHCP. Используйте форму **no** этой команды для удаления указанной записи.

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

### Параметры

<i>CLIENT-HARDWARE-ADDRESS</i>	(Опционально) Укажите MAC-адрес клиента.
--------------------------------	--

### По умолчанию

Нет

### Режим ввода команды

DHCP Server Screen Configure Mode

### Использование команды

Если запись привязки определена с MAC-адресом клиента, то сообщение сервера с указанным IP-адресом сервера и адресом клиента в полезной нагрузке будет разрешено. Эти записи привязки ограничивают, что только определенным серверам разрешено предлагать адреса для обслуживания определенных клиентов.

Если запись привязки определена без MAC-адреса клиента, то будет разрешено сообщение сервера с указанным IP-адресом сервера в полезной нагрузке. Эти записи привязки ограничивают возможность предоставления услуг сервера DHCP только определенным серверам.

### Пример

В этом примере показано, как настроить профиль экрана DHCP-сервера с именем "campus-profile", который содержит список MAC-адресов клиентов.

```
Switch# configure terminal
Switch(config)# dhcp-server-screen profile campus-profile
switch(config-dhcp-server-screen)# based-on hardware-address 00-08-01-02-03-04
switch(config-dhcp-server-screen)# based-on hardware-address 00-08-01-03-00-01
switch(config-dhcp-server-screen)#
```

## 16-18 clear ip dhcp snooping server-screen log

Эта команда используется для очистки буфера журнала экрана сервера.

**clear ip dhcp snooping server-screen log**

**Параметры**

Нет

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode.

**Использование команды**

Используйте эту команду для очистки буфера журнала экрана сервера. Буфер журнала экрана сервера DHCP отслеживает информацию о пакетах, которые не прошли проверку. Первый пакет, нарушивший проверку, будет отправлен в модуль журнала и записан в буфер журнала экрана сервера. Последующие пакеты, относящиеся к той же сессии, не будут отправляться в модуль регистрации, пока не будет очищена запись в буфере регистрации.

**Пример**

В этом примере показано, как очистить журнал экрана сервера.

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

**16- 19 dhcp-server-screen profile**

Эта команда используется для определения профиля экрана сервера и входа в режим настройки экрана сервера DHCP. Используйте форму **no** этой команды для удаления указанного профиля экрана сервера.

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

**Параметры**

<i>PROFILE-NAME</i>	Указывает имя профиля, содержащее не более 32 символов.
---------------------	---

**По умолчанию**

Нет

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Используйте эту команду для входа в режим настройки экрана сервера DHCP для определения профиля экрана сервера. Профиль можно использовать для определения записи экрана сервера DHCP.

## Пример

В данном примере показано, как войти в режим настройки экрана DHCP-сервера для определения профиля "campus".

```
Switch# configure terminal
Switch(config)# service dhcp
switch(config)# dhcp-server-screen profile campus
switch(config-dhcp-server-screen)#
```

## 16-20 ip dhcp snooping server-screen

Эта команда используется для включения проверки DHCP-сервера. Используйте форму **no** этой команды, чтобы отключить ее.

```
ip dhcp snooping server-screen [SERVER-IP-ADDRESS [profile PROFILE-NAME]]
no ip dhcp snooping server-screen [SERVER-IP-ADDRESS]
```

### Параметры

<i>PROFILE-NAME</i>	(Опционально) Указывает профиль со списком MAC-адресов клиентов для DHCP-сервера.
<i>SERVER-IP-ADDRESS</i>	(Опционально) Укажите IP-адрес доверительного DHCP-сервера.

### По умолчанию

Нет

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Функция отсеивания DHCP-сервера используется для фильтрации пакетов DHCP-сервера на определенном интерфейсе и получения доверительных пакетов от определенного источника. Эта функция может сделать защищенную сеть пригодной для использования, когда вредоносный узел отправляет пакеты DHCP-сервера.

Если IP-адрес сервера не указан, это включит или отключит экран DHCP-сервера на интерфейсе. По умолчанию экран DHCP-сервера отключен на всех интерфейсах. Если экран DHCP-сервера включен, на определенном интерфейсе он будет фильтровать все пакеты DHCP-сервера с интерфейса и пересылать только пакеты доверенного сервера.

Если запись экрана сервера определена с профилем, который содержит MAC-адрес клиента, то пересылается сообщение сервера с IP-адресом сервера и адресами клиентов, содержащимися в профиле.

Если запись определена без MAC-адреса клиента, то будет перенаправлено сообщение сервера с указанным IP-адресом сервера. Каждый сервер может иметь только одну соответствующую запись в таблице.

Если запись определена с профилем, но такой записи не существует, то сообщения с IP-адресом сервера, указанным этой записью, не пересылаются.

## Пример

В этом примере показано, как настроить профиль экрана сервера DHCP с именем "campus-profile" и связать его с записью экрана сервера DHCP на порту 3.

```
Switch# configure terminal
Switch(config)# dhcp-server-screen profile campus-profile
switch(config-dhcp-server-screen)# based-on hardware-address 00-08-01-02-03-04
switch(config-dhcp-server-screen)# based-on hardware-address 00-08-01-03-00-01
switch(config-dhcp-server-screen)# exit
switch(config)# interface eth1/0/3
switch(config-if)# ip dhcp snooping server-screen 10.1.1.2 profile campus-profile
switch(config-if)#
```

## 16-21 ip dhcp snooping server-screen log-buffer

Эта команда используется для настройки параметра буфера журнала экрана DHCP-сервера. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

**ip dhcp snooping server-screen log-buffer entries *NUMBER***  
**no ip dhcp snooping server-screen log-buffer entries**

### Параметры

<i>NUMBER</i>	Указывает номер записи в буфере. Максимальное число - 1024.
---------------	---

### По умолчанию

По умолчанию это значение равно 32.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте эту команду для настройки максимального количества записей в буфере журнала. Буфер журнала экрана сервера DHCP сохраняет информацию о пакетах, которые не прошли проверку. Первый пакет, нарушивший проверку, будет отправлен в модуль журнала и записан в буфер журнала экрана сервера. Последующие пакеты, принадлежащие той же сессии, не будут отправляться в модуль журнала, пока не будет очищена запись в буфере журнала.

Если буфер журнала заполнен, но происходит больше событий нарушения, пакеты будут отброшены, но событие не будет отправлено в модуль syslog. Если пользователь укажет размер буфера меньше, чем номер текущей записи, то буфер журнала будет автоматически очищен.

## Пример

В этом примере показано, как изменить максимальное число буферов на 64.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping server-screen log-buffer entries 64
Switch(config)#
```

## 16-22 show ip dhcp server-screen log

Эта команда используется для отображения буфера журнала экрана сервера.

**show ip dhcp server-screen log**

### Параметры

Нет

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте эту команду для отображения содержимого буфера журнала экранов DHCP-сервера. В буфере хранится информация о сообщениях сервера, нарушающих экранирование. Отслеживается количество повторений одного и того же нарушения и последнее время появления.

### Пример

В этом примере показано, как отобразить буфер журнала экрана сервера DHCP.

```
Switch# show ip dhcp server-screen log
Total log buffer size: 64

VLAN   Server IP      Client MAC      Occurrence
-----
100    10.20.1.1      00-20-30-40-50-60 06:30:37, 2014-03-10
100    10.58.2.30     10-22-33-44-50-60 06:31:42, 2014-03-10

Total Entries: 2

Switch#
```

## 16-23 snmp-server enable traps dhcp-server-screen

Эта команда используется для включения отправки SNMP-уведомлений для атаки forge DHCP Server. Для отключения отправки SNMP-уведомлений используйте форму **no** этой команды.

**snmp-server enable traps dhcp-server-screen**  
**no snmp-server enable traps dhcp-server-screen**

#### Параметры

Нет

#### По умолчанию

По умолчанию эта опция отключена.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Если включен экран сервера DHCP и коммутатор получает поддельный пакет сервера DHCP, коммутатор будет регистрировать событие, если получен какой-либо атакующий пакет. Вы можете использовать эту команду для включения или отключения отправки SNMP-уведомлений для таких событий.

#### Пример

В этом примере показано, как включить отправку ловушек для проверки DHCP-сервера.

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



## 17. Команды DHCPv6 Client

### 17-1 clear ipv6 dhcp client

Данная команда используется для перезапуска DHCPv6 Client на интерфейсе.

```
clear ipv6 dhcp client INTERFACE-ID
```

#### Параметры

<i>INTERFACE-ID</i>	Укажите интерфейс VLAN, для которого необходимо перезапустить DHCPv6 Client.
---------------------	--

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Эта команда доступна только для конфигурации интерфейса VLAN. Используйте эту команду для перезапуска клиента IPv6 DHCP на указанном интерфейсе.

#### Пример

В данном примере показано, как перезапустить DHCPv6 Client для интерфейса VLAN 1.

```
Switch# clear ipv6 dhcp client vlan 1
Switch#
```

### 17-2 show ipv6 dhcp

Данная команда используется для отображения настроек DHCPv6 на интерфейсе.

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

#### Параметры

<i>INTERFACE-ID</i>	Укажите интерфейс VLAN, для которого необходимо отобразить настройки DHCPv6.
---------------------	--

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

### Использование команды

Используйте данную команду, чтобы отобразить DHCPv6 DUID устройства, или используйте команду **show ipv6 dhcp interface**, чтобы отобразить настройки DHCPv6 для интерфейсов. Если ID интерфейса не указан, будут отображены все интерфейсы с функцией DHCPv6.

### Пример

В данном примере показано, как отобразить DHCPv6 DUID для устройства.

```
Switch# show ipv6 dhcp
This device's DUID is 0001000111A8040D001FC6D1D47B.
Switch#
```

В данном примере показано, как отобразить настройки DHCPv6 для интерфейса VLAN 1, если на VLAN 1 отключена функция DHCPv6.

```
Switch# show ipv6 dhcp interface vlan 1
vlan 1 is not in DHCPv6 mode.
Switch#
```

В данном примере показано, как отобразить настройки DHCPv6 для всех VLAN. Отображаются только те VLAN, на которых включена функция DHCPv6.

```
Switch# show ipv6 dhcp interface
vlan 1 is in client mode
State is OPEN
List of known servers:
  Reachable via address: FE80::200:11FF:FE22:3344
Configuration parameters:
  IA PD: IA ID 1, T1 40, T2 64
  Prefix: 2000::/48
         preferred lifetime 80, valid lifetime 100
Prefix name: yy
Rapid-Commit: disabled
Switch#
```

## 18. Команды DHCPv6 Guard

### 18-1 ipv6 dhcp guard policy

Данная команда используется для создания или изменения политики DHCPv6 Guard Policy. Команда позволяет войти в режим DHCPv6 Guard Configuration Mode. При использовании формы **no** данная команда удалит политику DHCPv6 Guard.

```
ipv6 dhcp guard policy POLICY-NAME
no ipv6 dhcp guard policy POLICY-NAME
```

#### Параметры

<i>POLICY-NAME</i>	Укажите имя политики DHCPv6 Guard.
--------------------	------------------------------------

#### По умолчанию

Нет

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Данная команда используется для создания или изменения политики DHCPv6 Guard Policy. Команда позволяет войти в режим DHCPv6 Guard Configuration Mode. Политики DHCPv6 Guard могут использоваться для блокировки ответов DHCPv6 Reply и сообщений, приходящих с неавторизованного сервера. Сообщения клиента не блокируются.

После создания политики DHCPv6 Guard используйте команду **ipv6 dhcp guard attach-policy** 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)#
```

### 18-2 device-role

Данная команда используется для указания роли подключенного устройства. При использовании формы **no** данная команда вернется к настройкам по умолчанию.

```
device-role {client | server}
no device-role
```

#### Параметры

<b>client</b>	Укажите, чтобы настроить подключенное устройство в качестве клиента DHCPv6. Все сообщения сервера DHCPv6 на этом порту будут отбрасываться.
<b>server</b>	Укажите, чтобы настроить подключенное устройство в качестве сервера DHCPv6. Все сообщения сервера DHCPv6 на этом порту будут приниматься.

**По умолчанию**

По умолчанию настроена опция **client**.

**Режим ввода команды**

DHCPv6 Guard Policy Configuration Mode

**Использование команды**

Данная команда используется для указания роли подключенного устройства. По умолчанию устройство выполняет роль клиента, и все сообщения сервера DHCPv6, приходящие на порт, будут отбрасываться. Если настроить устройство в качестве сервера, сообщения сервера DHCPv6 будут разрешены на данном порту.

**Пример**

В данном примере показано, как создать политику DHCPv6 Guard и настроить устройство в качестве сервера.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp guard policy dhcpguard1
Switch(config-dhcp-guard)# device-role server
Switch(config-dhcp-guard)#
```

**18-3 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**

<i>IPV6-ACCESS-LIST-NAME</i>	Укажите список доступа IPv6, с которым необходимо сверяться.
------------------------------	--

**По умолчанию**

По умолчанию опция отключена.

**Режим ввода команды**

DHCPv6 Guard Policy Configuration Mode

**Использование команды**

Данная команда используется для фильтрации 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 данном примере показано, как создать политику DHCPv6 Guard и настроить проверку соответствия адресов IPv6 со списком доступа list1.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp guard policy dhcp_filter1
Switch(config-dhcp-guard)# match ipv6 access-list list1
Switch(config-dhcp-guard)#
```

## 18-4 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

---

<i>POLICY-NAME</i>	(Опционально) Указывает имя политики защиты DHCPv6.
--------------------	---

---

### По умолчанию

По умолчанию опция отключена.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Данная команда используется для применения политики DHCPv6 Guard на интерфейсе. Политики DHCPv6 Guard используются для блокировки DHCPv6-сообщений сервера или фильтрации сообщений сервера на основе IP-адреса источника. Если имя политики не указано, то политика по умолчанию настроит устройство в качестве клиента.

### Пример

В этом примере показано применение политики защиты DHCPv6 "pol1" к порту 3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ipv6 dhcp guard attach-policy pol1
Switch(config-if)#
```

## 18-5 show ipv6 dhcp guard policy

Данная команда позволяет отобразить информацию о DHCPv6 Guard.

**show ipv6 dhcp guard policy [POLICY-NAME]****Параметры**

<i>POLICY-NAME</i>	(Опционально) Укажите имя политики DHCPv6 Guard.
--------------------	--

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Если параметр не указан, отображается информация обо всех политиках.

**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**

<b>Device Role</b>	Роль устройства. Ролью может быть клиент или сервер.
<b>Target</b>	Название интерфейса.
<b>Source Address Match Access List</b>	Список доступа IPv6 определенной политики.

## 19. Команды DHCPv6 Relay

### 19-1 ipv6 dhcp relay destination

Данная команда используется для того, чтобы включить DHCP для IPv6 Relay Service на интерфейсе и указать адрес назначения (destination), на который передаются сообщения клиентов. Используйте форму **no**, чтобы удалить Relay Destination.

```
ipv6 dhcp relay destination IPV6-ADDRESS [INTERFACE-ID]  
no ipv6 dhcp relay destination IPV6-ADDRESS
```

#### Параметры

<i>IPV6-ADDRESS</i>	Укажите адрес DHCPv6 Relay Destination.
<i>INTERFACE-ID</i>	(Опционально) Укажите выходной интерфейс для Relay Destination.

#### По умолчанию

По умолчанию данная опция отключена.

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

Чтобы включить на интерфейсе функцию DHCPv6 Relay, настройте адрес Relay Destination при помощи команды **ipv6 dhcp relay destination**. Чтобы удалить адрес Relay, используйте команду **no ipv6 dhcp relay destination**. При удалении всех адресов Relay функция Relay будет отключена.

Входящие сообщения DHCPv6, поступающие от клиента, могут быть заранее ретранслированы при помощи Relay Agent. Адрес назначения, который необходимо ретранслировать, может принадлежать DHCPv6-серверу или другому DHCPv6 Relay Agent.

В качестве адреса назначения может быть использован индивидуальный или групповой адрес, оба могут быть как Link Scoped, так и Global Scoped. Для адресов Link Scoped необходимо указать интерфейс, в котором расположен адрес назначения. Для адресов Global Scoped можно указать выходной интерфейс (опционально). Если выходной интерфейс не указан, он определяется при помощи таблицы маршрутизации.

Для одного интерфейса можно указать несколько адресов Relay Destination. Если сообщение DHCPv6 ретранслируется на групповой адрес, для поля Hop Limit в заголовке пакета IPv6 будет установлено значение 32.

#### Пример

В этом примере показано, как настроить адрес назначения реле на VLAN 1 и VLAN 2.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 vlan 1
Switch(config-if)# ipv6 dhcp relay destination FE80::22:33 vlan 2
Switch(config-if)#
```

## 19-2 ipv6 dhcp relay remote-id format

Данная команда используется для настройки sub-опции Remote ID. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**ipv6 dhcp relay remote-id format {cid-with-user-define | default | expert-udf | user-define}**  
**no ipv6 dhcp relay remote-id format**

### Параметры

#### default

Укажите, чтобы использовать системный MAC-адрес коммутатора в качестве Remote ID. Формат Remote ID представлен ниже:

F01	F02	F03	F04	F05
Sub Type	VLAN ID	Module ID	Port ID	MAC Address
1 byte	2 bytes	1 byte	1 byte	6 bytes

**F01. Tun sub-опции:** число 1 свидетельствует о том, что тип данного ID – Remote ID.

**F02. VLAN ID:** входящий VLAN ID в пакете DHCP Client.

**F03. ID модуля:** ID модуля для автономных коммутаторов – O.ID модуля для стекированных коммутаторов – Unit ID.

**F04. ID порта:** номер входящего порта в пакете DHCP Client.

Номера портов начинаются с 1.

**F05. MAC-адрес:** системный MAC-адрес коммутатора.

#### cid-with-user-define

Укажите, чтобы использовать CID со строкой, заданной пользователем, в качестве Remote ID. Формат Remote ID представлен ниже:

F01	F02	F03	F04	F05
Sub Type	VLAN ID	Module ID	Port ID	User Defined
1 byte	2 bytes	1 byte	1 byte	Max. 256 bytes

**F01. Tun sub-опции:** число 2 свидетельствует о том, что тип данного ID – Remote ID.



---

**F02. VLAN ID:** входящий VLAN ID в пакете DHCP Client.

**F03. ID модуля:** ID модуля для автономных коммутаторов – 0.

ID модуля для стекированных коммутаторов – Unit ID.

**F04. ID порта:** номер входящего порта в пакете DHCP Client.

Номера портов начинаются с 1.

**F05. Задать самостоятельно:** заданная пользователем строка, настраиваемая при помощи команды **ipv6 dhcp relayremote-id udf**. По умолчанию данное поле не заполнено.

---

#### user-define

Укажите, чтобы задать Remote ID самостоятельно. Формат Remote ID представлен ниже:

```
|-----|
| F01      | F02      |
|-----|-----|
| Sub Type  | User Defined |
|-----|-----|
| 1 byte    | Max. 256 bytes |
|-----|
```

**F01. Tun sub-опции:** число 3 свидетельствует о том, что тип данного ID – Remote ID.

**F02. Задать самостоятельно:** заданная пользователем строка, настраиваемая при помощи команды **ipv6 dhcp relayremote-id udf**.

---

#### expert-udf

Указывает на использование гибкой строки, определяемой пользователем, в качестве удаленного ID. Опция удаленного ID формируется в следующем формате:

```
|-----|
| F01      |
|-----|
| User Defined |
|-----|
| Max. 256 bytes |
|-----|
```

**F01. Определено пользователем:** Гибкая пользовательская строка, настроенная в командах **ipv6 dhcp relay remote-id format-type**, **ipv6 dhcp relay remote-id profile** и **format string**. По умолчанию поле пустое.

---

По умолчанию

Нет

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте данную команду, чтобы настроить sub-опцию Remote ID.

#### Пример

В данном примере показано, как настроить sub-опцию Remote ID «cid-with-user-define».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id format cid-with-user-define
Switch(config)#
```

### 19-3 ipv6 dhcp relay remote-id option

Данная команда используется для того, чтобы включить встраивание Relay Agent Remote ID Option 37 в ретранслируемых пакетах запроса DHCP IPv6. Используйте форму **no**, чтобы отключить данную функцию.

```
ipv6 dhcp relay remote-id option
no ipv6 dhcp relay remote-id option
```

#### Параметры

Нет

#### По умолчанию

По умолчанию данная опция отключена.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте данную команду, чтобы включить встраивание функции DHCPv6 Relay Agent Remote ID Option.

#### Пример

В данном примере показано, как включить встраивание DHCPv6 Relay Agent Remote ID Option.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id option
Switch(config)#
```

### 19-4 ipv6 dhcp relay remote-id policy

Данная команда используется для настройки политики перенаправления Option 37 для DHCPv6 Relay Agent. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ipv6 dhcp relay remote-id policy {drop | keep}
no ipv6 dhcp relay remote-id policy
```

#### Параметры

<b>drop</b>	Укажите, чтобы отбросить пакет, в котором уже есть Relay Agent Remote ID Option 37.
<b>keep</b>	Укажите, чтобы напрямую ретранслировать пакет запроса DHCPv6, в котором уже есть Relay Agent Remote ID Option, на сервер DHCPv6 в неизменном виде.

#### По умолчанию

Параметр по умолчанию – **keep**.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте данную команду, чтобы настроить глобальную политику для пакетов, в которых уже есть Option 37. При выборе политики **drop** полученный от клиента пакет, в котором уже присутствует RelayAgent Remote ID Option, будет отброшен. При выборе политики **keep** коммутатор не будет проверять, присутствует ли в полученном пакете Relay Agent Remote ID Option.

#### Пример

В данном примере показано, как настроить политику DHCPv6 Relay Agent Remote ID Option так, чтобы пакет был отброшен при наличии в нем Relay Agent Remote ID Option.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id policy drop
Switch(config)#
```

## 19-5 ipv6 dhcp relay remote-id profile

Эта команда используется для создания нового профиля для DHCPv6 relay Option 37 и входа в режим конфигурации профиля DHCPv6. Для удаления профиля используйте форму **no** этой команды.

```
ipv6 dhcp relay remote-id profile NAME
no ipv6 dhcp relay remote-id profile NAME
```

#### Параметры

<b>NAME</b>	Указывает имя профиля. Максимальная длина - 32 символа. В профиле может быть создано до 6 записей.
-------------	--

**По умолчанию**

Нет

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Используйте эту команду, чтобы создать или удалить профиль для DHCPv6 relay Option 37 или войти в режим конфигурации профиля DHCPv6.

**Пример**

В этом примере показано, как создать профиль profile1 для DHCPv6 relay Option 37.

```
Switch#configure configure terminal
Switch(config)#ipv6 dhcp relay remote-id profile profile1
Switch(config-dhcp-profile)#
```

**19-6 format string**

Эта команда используется для отмены ввода flexible user-defined Option 18 or Option 37. Используйте форму **no** этой команды для удаления записи flexible user-defined Option 18 or Option 37.

**format string** *STRING*  
**no format string**

**Параметры****Параметры**

<i>STRING</i>	<p>Укажите формат Option 82 DHCP. Максимально допустимое количество символов – 255.</p> <p>Ниже представлены правила конфигурирования данного параметра:</p> <ul style="list-style-type: none"> <li>• Параметр может содержать шестнадцатеричные значения, строку ASCII или любую комбинацию шестнадцатеричных значений и строки ASCII. Строка ASCII должна быть заключена в кавычки (" "), например:"Ethernet". Символы ASCII вне кавычек будут распознаны как шестнадцатеричные значения.</li> <li>• Отформатированная ключевая строка – строка, которую необходимо преобразовать до того, как она будет запакетирована. Отформатированная ключевая строка может содержать как строки ASCII, так и шестнадцатеричные значения, например: "%"+ "\$"+ "1- 32"+ "keyword"+ ":%" – указывает на то, что строка, следующая за символом, является отформатированной ключевой строкой.</li> </ul>
---------------	--

**\$** или **0** – (опционально) индикатор заполнения.

Данная опция указывает, как заполнить отформатированную ключевую строку в соответствии с требованиями по длине строки. Значение данной опции – \$ или 0.

**\$** означает заполнение начального пробела (0x20). **0** означает заполнение начального нуля (**0**). Заполнение начального нуля – настройка по умолчанию.

**1-32** – (опционально) индикатор длины. Данная опция указывает, сколько символов или байтов должна занимать преобразованная ключевая строка. Если фактическая длина транслируемой ключевой строки меньше длины, предусмотренной данной опцией, будет использован индикатор заполнения. В других случаях будет использована фактическая длина строки.

**keyword** -ключевое слово будет преобразовано на основе фактического значения системы. Следующие ключевые слова указывают, что команда будет отклонена при обнаружении неизвестных или неподдерживаемых ключевых слов:

**devtype:** модель устройства. Выводится из поля Module Name в команде **show version**. Допустимо использование только строки ASCII.

**sysname:** системное имя коммутатора. Максимально допустимое количество символов – 128. Допустимо использование только строки ASCII.

**ifdescr:** выводится из ifDescr (IF-MIB). Допустимо использование только строки ASCII.

**portmac:** MAC-адрес порта. Могут быть использованы строка ASCII или шестнадцатеричные значения. При использовании строки ASCII MAC-адрес может быть настроен с помощью специальной команды (например, **ip dhcp relay information option mac-format case**). При использовании шестнадцатеричных значений MAC-адрес будет сформирован в шестнадцатеричном виде.

**sysmac:** системный MAC-адрес. Могут быть использованы строка ASCII или шестнадцатеричные значения. При использовании строки ASCII MAC-адрес может быть сформирован при помощи команд CLI (например, **ip dhcp relay information option mac-format case**). При использовании шестнадцатеричных символов MAC-адрес будет сформирован в шестнадцатеричном виде.

**unit:** Unit ID коммутатора в стеке. Могут быть использованы строка ASCII или шестнадцатеричные значения. Для

---

нестекированных коммутаторов ID указывается при помощи команды **ip dhcp relay information option format remote-id expert-udf [standalone\_unit\_format {0 | 1}]**, а также команды **ipdhcp relay information option format circuit-id expert-udf [standalone\_unit\_format {0 | 1}]**.

**module:** ID модуля. Могут быть использованы строка ASCII или шестнадцатеричные значения.

**port:** номер локального порта. Могут быть использованы строка ASCII или шестнадцатеричные значения.

**svlan:** ID внешней VLAN. Могут быть использованы строка ASCII или шестнадцатеричные значения.

**cvlan:** ID внутренней VLAN. Могут быть использованы строка ASCII или шестнадцатеричные значения.

**:** - конец отформатированной ключевой строки. Если отформатированная ключевая строка является последним параметром команды, ее заключительный символ (:) может быть игнорирован. Пробел (0x20) между % и : будет игнорирован. Другие пробелы будут включены.

- Строки ASCII могут содержать любые комбинации отформатированных ключевых строк, символов 0-9, a-z, A-Z, !, @, #, \$, %, ^, &, \*, (, ), \_, +, |, -, =, \, [, ], {, }, ;, :, ', ", /, ., ,, <, >, ` и пробелов. \ используется в качестве знака перехода. Специальные символы после \ являются самостоятельными символами. Например, % в комбинации \% является самостоятельным символом, а не индикатором запуска отформатированной ключевой строки. Пробелы вне отформатированной ключевой строки также будут включены.
- Шестнадцатеричные значения могут содержать любые комбинации отформатированных ключевых строк, символов 0-9, A-F, a-f и пробелов. Отформатированные ключевые строки поддерживают только те ключевые слова, в которых используются шестнадцатеричные значения. Пробелы вне отформатированной ключевой строки включены не будут.

#### По умолчанию

Нет

#### Режим ввода команды

DHCP Profile Mode

#### Использование команды

Используйте эту команду для настройки ввода flexible user-defined Option 18 или Option 37.

## Пример

В этом примере показано, как настроить ввод flexible user-defined Option 18.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id profile profile1
Switch(config-dhcp-profile)#format string "%port:\:%sysname:%05svlan"
Switch(config-dhcp-profile)#
```

## 19-7 ip dhcp relay information option mac-format case

Эта команда используется для определения формата MAC-адреса flexible user-defined profile DHCPv6 Option 18 или Option 37. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

```
ip dhcp relay information option mac-format case {lowercase | uppercase} delimiter {hyphen | colon | dot | none} number {1 | 2 | 5}
no ip dhcp relay information option mac-format case
```

### Параметры

<b>lowercase</b>	Указывает, что при использовании формата в нижнем регистре MAC-адрес опции 18 или опции 37 для определяемого пользователем профиля будет иметь формат: aa-bb-cc-dd-ee-ff.
<b>uppercase</b>	Указывает, что при использовании формата с заглавными буквами MAC-адрес опции 18 или опции 37 для имени пользователя профиля, определяемого пользователем, будет иметь следующий вид: AA-BB-CC-DD-EE-FF.
<b>hyphen</b>	Укажите, чтобы использовать «-» в качестве разделителя данных: AA-BB-CC-DD-EE-FF.
<b>colon</b>	Укажите, чтобы использовать «:» в качестве разделителя данных: AA:BB:CC:DD:EE:FF.
<b>dot</b>	Укажите, чтобы использовать «.» в качестве разделителя данных: AA.BB.CC.DD.EE.FF.
<b>none</b>	Укажите для ввода данных без разделителя: AABVCCDDEEFF.
<b>number</b>	Укажите количество разделителей: <b>1:</b> один разделитель: AABVCC.DDEEFF. <b>2:</b> два разделителя: AABV.CCDD.EEFF. <b>5:</b> несколько разделителей: AA.BB.CC.DD.EE.FF. Если указан параметр none, параметр number будет недействителен.

### По умолчанию

Параметр регистра MAC-адреса аутентификации по умолчанию – **uppercase**.

Параметр разделителя MAC-адреса аутентификации по умолчанию – **none**.

### Режим ввода команды

Global Configuration Mode

## Использование команды

Используйте эту команду для настройки формата MAC-адреса flexible user- defined profile DHCPv6 Option 18 или Option 37.

## Пример

В этом примере показано, как указать формат MAC-адреса гибкого пользовательского профиля Option 18 или Option 37.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay information option mac-format case uppercase delimiter hyphen
number 5
Switch(config)#
```

## 19-8 show ipv6 dhcp relay information option mac-format

Эта команда используется для отображения формата MAC-адреса профиля Option 18 и Option 37.

```
show ipv6 dhcp relay information option mac-format
```

## Параметры

Нет

## По умолчанию

Нет

## Режим ввода команды

EXEC Mode

## Использование команды

Используйте эту команду для отображения формата MAC-адреса профиля Option 18 и Option 37.

## Пример

В этом примере показано, как отобразить формат MAC-адреса для профиля Option 18 и Option 37.

```
Switch# show ipv6 dhcp relay information option mac-format

Case           : Uppercase
Delimiter      : Hyphen
Delimiter Number : 5
Example        : AA-BB-CC-DD-EE-FF

Switch#
```



## 19-9 ipv6 dhcp relay remote-id udf

Используйте данную команду, чтобы настроить User Define Field (UDF) для Remote ID. Используйте форму **no**, чтобы удалить запись UDF.

```
ipv6 dhcp relay remote-id udf {ascii STRING | hex HEX-STRING}
no ipv6 dhcp relay remote-id udf
```

### Параметры

<b>ascii</b> <i>STRING</i>	Укажите строку ASCII для UDF Remote ID. Максимально допустимое количество символов – 128.
<b>hex</b> <i>HEX-STRING</i>	Укажите шестнадцатеричную строку для UDF Remote ID. Максимально допустимое количество знаков – 256.

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду, чтобы настроить UDF для Remote ID.

### Пример

В данном примере показано, как настроить UDF (строка ASCII) «PARADISE001».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id udf ascii PARADISE001
Switch(config)#
```

В данном примере показано, как настроить UDF (шестнадцатеричная строка) «010c08».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id udf hex 010c08
Switch(config)#
```

## 19-10 ipv6 dhcp local-relay vlan

Эта команда используется для включения локальной ретрансляции DHCPv6 в сети VLAN или группе сетей VLAN. Используйте форму по этой команды для отключения функции.

```
ipv6 dhcp local-relay vlan VLAN-ID [, | -]
no ipv6 dhcp local-relay vlan VLAN-ID [, | -]
```

### Параметры

<i>VLAN-ID</i>	Указывает VLAN или диапазон VLAN.
,	(Опционально) Указывает серию сетей VLAN или отделяет диапазон сетей VLAN от предыдущего диапазона. До или после запятой пробел не допускается.
-	(Опционально) Указывает диапазон сетей VLAN. До или после дефиса пробел не допускается.

**По умолчанию**

По умолчанию этот параметр отключен.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Используйте эту команду для настройки функции локальной ретрансляции DHCPv6.

Когда функция локальной ретрансляции DHCPv6 включена, коммутатор будет добавлять Option 37 и Option 18 к пакетам запроса от клиента.

Если состояние проверки опции 37 включено, коммутатор будет проверять пакет запроса от клиента и отбрасывать пакет, если он содержит опцию 37, как указано в функции ретрансляции DHCPv6.

Если состояние проверки опции 37 отключено, функция локальной ретрансляции всегда будет добавлять опцию 37 в пакет запроса, независимо от того, включено или отключено состояние опции 37.

Функция локальной ретрансляции DHCPv6 будет напрямую пересылать пакет от сервера к клиенту, после чего дальнейшая обработка не производится.

**Пример**

В этом примере показано, как включить функцию локальной ретрансляции DHCPv6 в сети VLAN 100.

```
Switch# configure terminal
Switch(config)#ipv6 dhcp local-relay vlan 100
Switch(config)#
```

**19-11 show ipv6 dhcp**

Данная команда используется для отображения настроек DHCPv6 на интерфейсе.

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

**Параметры**

<i>INTERFACE-ID</i>	(Опционально) Укажите ID интерфейса VLAN, который
---------------------	---

---

необходимо отобразить.

---

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте данную команду, чтобы отобразить DHCPv6 DUID устройства. Для отображения настроек DHCPv6 и информации об указанном интерфейсе VLAN используйте команду **show ipv6 dhcp interface**. Если ID интерфейса не указан, будут отображены все интерфейсы, для которых включена функция DHCPv6.

**Пример**

В данном примере показано, как отобразить настройки DHCPv6 для VLAN 1, если режим DHCPv6 Relay Mode включен.

```
Switch # show ipv6 dhcp interface vlan1

vlan1 is in relay mode
  Relay destinations:
    FE80::20A:BBFF:FECC:102 via vlan2

Switch #
```

В данном примере показано, как отобразить информацию о DHCPv6 для интерфейса VLAN 1, если режим DHCPv6 Mode отключен.

```
Switch# show ipv6 dhcp interface vlan1

Vlan1 is not in DHCPv6 mode

Switch#
```

**19-12 show ipv6 dhcp relay information option**

Данная команда используется для отображения настроек DHCPv6 Relay Information Options.

**show ipv6 dhcp relay information option**

**Параметры**

Нет

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте данную команду, чтобы отобразить настройки DHCPv6 Relay Information Options.

**Пример**

В данном примере показано, как отобразить настройки DHCPv6 Relay Remote ID.

```
Switch# show ipv6 dhcp relay information option

IPv6 DHCP relay remote-id
Policy : drop
Format : user-define
UDF is ascii string "userstring"

Switch#
```

**19-13 show ipv6 dhcp relay remote-id profile**

Эта команда используется для отображения профилей Option 37.

**show ipv6 dhcp relay remote-id profile**

**Параметры**

Нет

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте эту команду для отображения профилей Option 37.

**Пример**

В этом примере показано, как отобразить профили Option 37.

```
Switch# show ipv6 dhcp relay remote-id profile

Option37 Profile name: profile1
Format string: "Ethernet %unit:/0/ %port:\:%sysname:%05svlan"

Total Entries:1

Switch#
```

## 19-14 show ipv6 dhcp relay information option format-type

Эта команда используется для отображения типа формата опций информации о ретрансляции DHCPv6.

**show ipv6 dhcp relay information option format-type [interface *INTERFACE-ID* [, | -]]**

### Параметры

<b>interface</b> <i>INTERFACE-ID</i>	(Опционально) Укажите интерфейсы, которые будут отображаться.
,	(Опционально) Указывает серию интерфейсов или отделяет диапазон интерфейсов от предыдущего диапазона. До или после запятой пробел не допускается.
-	(Опционально) Указывает диапазон интерфейсов. До или после дефиса пробел не допускается.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте эту команду для отображения типа формата опций информации о ретрансляции DHCPv6.

### Пример

В этом примере показано, как отобразить тип формата опций информации о ретрансляции DHCPv6.

```
Switch# show ipv6 dhcp relay information option format-type
```

```
eth1/0/1
```

```
Remote ID bind profile: 1
```

```
Total Entries: 1
```

```
Switch#
```

## 20. Команды клиента D-Link Discovery Protocol (DDP)

### 20-1 ddp

Данная команда используется для того, чтобы включить функцию клиента DDP глобально или на указанных портах. Используйте форму **no**, чтобы отключить функцию клиента DDP.

**ddp**  
**no ddp**

#### Параметры

Нет

#### По умолчанию

По умолчанию данная опция отключена.

#### Режим ввода команды

Global Configuration Mode  
Interface Configuration Mode

#### Использование команды

Используйте данную команду, чтобы включить/отключить функцию клиента DDP глобально или на физическом порту.

Если на порту отключена функция DDP, данный порт не будет ни обрабатывать, ни генерировать DDP-сообщения. Полученные портом DDP-сообщения распространяются в рамках широковещательного домена.

#### Пример

В данном примере показано, как включить DDP глобально.

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

В данном примере показано, как включить DDP на порту 1/0/1.

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

### 20-2 ddp report-timer

Данная команда используется для настройки интервала между двумя последовательными сообщениями DDP Report. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

**no ddp report-timer****Параметры**

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

**По умолчанию**

По умолчанию этот параметр равен 30 секундам.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Используйте данную команду, чтобы настроить интервал между двумя последовательными сообщениями DDP Report.

**Пример**

В данном примере показано, как установить интервал 60 секунд.

```
Switch# configure terminal
Switch(config)# ddp report-timer 60
Switch(config)#
```

**25-3 show ddp**

Данная команда используется для отображения настроек DDP на коммутаторе.

**show ddp [interfaces {INTERFACE-ID [, | -]}]**

**Параметры**

<i>INTERFACE-ID</i>	Укажите interface ID.
,	(Опционально) Указывает серию интерфейсов или отделяет диапазон интерфейсов от предыдущего диапазона. До или после запятой пробел не допускается.
-	(Опционально) Указывает диапазон интерфейсов. До или после дефиса пробел не допускается.

**По умолчанию**

Нет

**Режим ввода команды**



EXEC Mode

### Использование команды

Используйте данную команду, чтобы отобразить информацию о DDP на коммутаторе.

### Пример

В данном примере показано, как отобразить общую информацию о DDP.

```
Switch# show ddp

D-Link Discovery Protocol state: Enabled
Report timer: 60 seconds

Switch#
```

В данном примере показано, как отобразить информацию о DDP на порту 1/0/1.

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

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

Switch#
```

## 21. Команды Domain Name System (DNS)

### 21-1 clear host

Данная команда используется для удаления динамически изученных записей узла в режиме Privileged User Mode.

```
clear host {all} [HOST-NAME]}
```

#### Параметры

<b>all</b>	Укажите, чтобы удалить все записи узла.
<i>HOST-NAME</i>	(Опционально) Укажите, чтобы удалить указанную динамически изученную запись узла.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте данную команду, чтобы удалить запись узла или все записи узла, которые динамически изучены DNS Resolver или Caching Server.

#### Пример

В данном примере показано, как удалить динамически изученную запись «www.abc.com» из таблицы узлов.

```
Switch# clear host www.abc.com
Switch#
```

### 21-2 ip domain lookup

Данная команда используется для включения DNS, что позволяет использовать функцию Domain Name Resolution. Используйте форму **no**, чтобы отключить данную функцию.

```
ip domain lookup
no ip domain lookup
```

#### Параметры

Нет

#### По умолчанию

По умолчанию данная функция отключена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте команду **ip domain lookup**, чтобы включить функцию Domain Name Resolution. DNS Resolver отправляет запрос на указанный Name Server. Ответ, отсылаемый Name Server, будет кэширован и использован для ответа на последующие запросы.

### Пример

В данном примере показано, как включить функцию Domain Name Resolution.

```
Switch# configure terminal
Switch(config)# ip domain lookup
Switch(config)#
```

## 21-3 ip host

Данная команда используется для настройки статической записи привязки для имени узла, а также IP-адреса в таблице узлов. Используйте форму **no**, чтобы удалить статическую запись узла.

```
ip host HOST-NAME {IP-ADDRESS | IPV6-ADDRESS}
no ip host HOST-NAME {IP-ADDRESS | IPV6-ADDRESS}
```

### Параметры

<i>HOST-NAME</i>	Укажите имя узла устройства.
<i>IP-ADDRESS</i>	Укажите IPv4-адрес устройства.
<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес устройства.

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

Имя узла, указанное в этой команде, должно быть подходящим. Чтобы удалить статическую запись узла, используйте форму **no** данной команды.

### Пример

В данном примере показано, как настроить запись привязки имени узла «www.abc.com» и IP-адреса 192.168.5.243.

```
Switch# configure terminal
Switch(config)# ip host www.abc.com 192.168.5.243
Switch(config)#
```

## 21-4 ip name-server

Данная команда используется для настройки IP-адреса Domain Name Server. Используйте форму **no**, чтобы удалить сконфигурированный Domain Name Server.

```
ip name-server {IP-ADDRESS | IPV6-ADDRESS} [{IP-ADDRESS2 | IPV6-ADDRESS2}]
no ip name-server {IP-ADDRESS | IPV6-ADDRESS} [{IP-ADDRESS2 | IPV6-ADDRESS2}]
```

### Параметры

<i>IP-ADDRESS</i>	Укажите IPv4-адрес Domain Name Server.
<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес Domain Name Server.
<i>IP-ADDRESS2</i>	Укажите второй адрес IPv4 для сервера доменных имен.
<i>IPV6-ADDRESS2</i>	Укажите второй IPv6-адрес для сервера доменных имен.

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте эту команду для настройки сервера DNS. Если система не может получить ответ от DNS-сервера, она будет пытаться использовать следующий сервер до тех пор, пока не получит ответ. Если серверы имен уже настроены, серверы, настроенные позже, будут добавлены в список серверов. Можно указать два сервера имен IPv4/IPv6.

### Пример

В данном примере показано, как сконфигурировать Domain Name Server 192.168.5.134 и 5001:5::2.

```
Switch# configure terminal
Switch(config)# ip name-server 192.168.5.134 5001:5::2
Switch(config)#
```

## 21-5 ip name-server timeout

Данная команда используется для конфигурации значения тайм-аута для Name Server. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip name-server timeout SECONDS
no ip name-server timeout
```

**Параметры**

<i>SECONDS</i>	Укажите максимальное время ожидания ответа от указанногоName Server. Доступный диапазон значений: от 1 до 60 секунд.
----------------	--

**По умолчанию**

Значение по умолчанию – 3 секунды.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Используйте данную команду, чтобы настроить максимальное значение времени ожидания ответа от указанного Name Server.

**Пример**

В данном примере показано, как указать значение тайм-аута 5 секунд.

```
Switch# configure terminal
Switch(config)# ip name-server timeout 5
Switch(config)#
```

**21-6 show hosts**

Данная команда используется для отображения настроек DNS.

**show hosts****Параметры**

Нет

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте данную команду, чтобы отобразить информацию о настройках DNS.

**Пример**

В данном примере показано, как отобразить информацию о настройках DNS.

```
Switch#show hosts

Number of Static Entries: 1
Number of Dynamic Entries: 0

Host Name:      www.abc.com
IP Address:     192.168.5.243
Age:           forever

Switch#
```

## 26-7show ip name-server

Данная команда используется для отображения текущих DNS.

**show ip name-server**

### Параметры

Нет

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте данную команду, чтобы отобразить DNS.

### Пример

В этом примере показано, как отобразить информацию о конфигурации, связанную с DNS.

```
Switch# show ip name-server

Static name server:
192.168.5.134
5001:5::2

Dynamic name server:

Switch#
```



## 22. Команды предотвращения атак DoS

### 22-1 dos-prevention

Данная команда используется для включения и настройки механизма предотвращения атак DoS (DoS Prevention). При использовании формы **no** данная команда вернется к настройкам по умолчанию.

**dos-prevention** *DOS-ATTACK-TYPE*  
**no dos-prevention** *DOS-ATTACK-TYPE*

#### Параметры

<i>DOS-ATTACK-TYPE</i>	Укажите строку, идентифицирующую тип DoS, который необходимо настроить.
------------------------	---

#### По умолчанию

По умолчанию все поддерживаемые типы DoS отключены.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Данная команда используется для включения и настройки механизма предотвращения атак DoS для определенного типа атак DoS или для всех поддерживаемых типов. Механизмы предотвращения атак DoS (сопоставление и принятие мер) являются функциями аппаратного обеспечения.

При включенном предотвращении атак DoS коммутатор сохранит событие (лог) в журнале, если был получен хотя бы один «атакующий» пакет.

Команда **no dos-prevention** с ключевым словом **all** используется для отключения механизма предотвращения атак DoS для всех поддерживаемых типов. Все настройки будут возвращены к значениям по умолчанию для определенных типов атак.

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

- **Blat:** данный тип атаки включает в себя отправку устройству пакетов с портом источника TCP/UDP, равным порту назначения. Это может послужить причиной того, что устройство будет отвечать самому себе.
- **Land:** атака LAND включает в себя отправку устройству IP-пакетов с адресом источника и назначения, равным адресу устройства. Это может послужить причиной того, что устройство будет непрерывно отвечать самому себе.
- **TCP-NULL-scan:** сканирование порта с использованием определенных пакетов, содержащих последовательность чисел от 0 и не содержащих флаги.
- **TCP-SYN-fin:** сканирование порта с использованием определенных пакетов, содержащих флаги SYN и FIN.
- **TCP-xmas-scan:** сканирование порта с использованием определенных пакетов, содержащих последовательность чисел от 0 и флаги Urgent (URG), Push (PSH) и FIN.
- **Ping-death:** данный тип атаки на компьютер включает в себя отправку некорректного или вредоносного ping-запроса компьютеру. Обычно размер ping-запроса составляет 64 байта; многие



компьютеры не могут распознать ping-запрос, если он больше, чем максимальный размер IP-пакета (65535 байт). Отправка ping-запроса такого размера может повредить компьютер назначения. Как правило, данным сбоем можно относительно просто воспользоваться. Отправка ping-пакета размером 65536 байт недопустима согласно сетевому протоколу, но пакет такого размера можно отправить, если он будет фрагментирован. При повторной сборке пакета буфер компьютера может переполниться, что послужит причиной сбоя системы.

- **TCP-tiny-frag**: при атаке Tiny TCP Fragment используется фрагментация IP для создания очень маленьких фрагментов, чтобы TCP-заголовок был в отдельном фрагменте пакета. Это позволяет ему обойти проверку маршрутизатора и выполнить атаку.
- **All**: все вышеперечисленные типы.
- **TCP-syn-rst** - TCP-пакет с флагами TCP SYN и RST, которые являются незаконными и потенциально угрожают безопасности.
- **Smurf** - Атакующий посылает большое количество пакетов ICMP-запросов на широковещательный IP-адрес, IP-адрес источника атакующих пакетов равен IP-адресу жертвы. Если маршрутизатор доставляет трафик на широковещательный IP-адрес, все узлы в этой IP-сети ответят ICMP на IP-адрес жертвы.

### 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)#
```

## 22-2 show dos-prevention

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

**show dos-prevention [DOS-ATTACK-TYPE]**

### Параметры

<i>DOS-ATTACK-TYPE</i>	(Опционально) Укажите тип DoS, который необходимо отобразить.
------------------------	---

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

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

### Пример

В данном примере показан процесс вызова информации о настройках предотвращения атак DoS.

```
Switch#show dos-prevention

DoS Prevention Information
DoS Type                State
-----
Land Attack             Enabled
Blat Attack             Enabled
TCP Null                Disabled
TCP Xmas                Disabled
TCP SYN-FIN            Disabled
TCP SYN SrcPort Less 1024 Disabled
Ping of Death Attack   Disabled
TCP Tiny Fragment Attack Disabled

Switch#
```

В данном примере показан процесс вызова информации о настройках предотвращения атак DoS для типа атаки Land.

```
Switch#show dos-prevention land

DoS Type : Land Attack
State    : Enabled

Switch#
```

## 22-3 snmp-server enable traps dos-prevention

Данная команда используется для отправки SNMP-уведомлений о DoS-атаках. Для отключения данной команды используйте форму **no**.

```
snmp-server enable traps dos-prevention
no snmp-server enable traps dos-prevention
```

### Параметры

Нет

### По умолчанию

По умолчанию данная функция отключена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Если предотвращение атак DoS включено, каждые пять минут коммутатор будет записывать в журнал событие, если какой-либо атакующий пакет будет принят за этот промежуток времени. Используйте данную команду, чтобы включить или отключить отправку уведомлений SNMP для таких событий.

### Пример

В данном примере показано, как включить отправку трапов для атак DoS.

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

---

## 23. Команды Dynamic ARP Inspection

### 23-1 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

<i>NAME</i>	Укажите имя списка доступа ARP, который необходимо настроить. Максимальная допустимая длина – 32 символа.
-------------	--

#### По умолчанию

Нет

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Имя должно быть уникальным среди всех списков доступа. Имя чувствительно к регистру. В конце списка доступа указан запрет в доступе всем, кого нет в списке разрешений.

#### Пример

В данном примере показано, как настроить список доступа ARP с двумя разрешающими записями.

```
Switch# configure terminal
Switch(config)# arp access-list static-arp-list
Switch(config-arp-nacl)# permit ip 10.20.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)# permit ip 10.30.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)#
```

### 23-2 clear ip arp inspection log

Данная команда используется для очистки буфера журнала ARP Inspection.

```
clear ip arp inspection log
```

#### Параметры

Нет

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Данная команда используется для очистки буфера журнала ARP Inspection.

**Пример**

В данном примере показано, как очистить журнал ARP Inspection.

```
Switch# clear ip arp inspection log
Switch#
```

**23-3 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**

<b>all</b>	Укажите для удаления данных статистики Dynamic ARP Inspection для всех VLAN.
<b>vlan VLAN-ID</b>	Укажите VLAN или диапазон VLAN.
<b>,</b>	(Опционально) Выделение серии VLAN или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
<b>-</b>	(Опционально) Выделение диапазона VLAN. Пробелы до и после дефиса недопустимы.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Данная команда используется для удаления данных статистики Dynamic ARP Inspection.

**Пример**

В данном примере показано, как удалить данные статистики Dynamic ARP Inspection для VLAN 1.

```
Switch# clear ip arp inspection statistics vlan 1
Switch#
```

## 23-4 ip arp inspection filter vlan

Данная команда используется для указания списка доступа ARP, который будет использоваться для проверки ARP Inspection для VLAN. При использовании формы **no** команда удалит указанную привязку.

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

### Параметры

<i>ARP-ACL-NAME</i>	Указывает имя списка управления доступом. Максимальная допустимая длина – 32 символа.
<b>vlan</b> <i>VLAN-ID</i>	Укажите VLAN, сопоставленную со списком доступа ARP.
,	(Опционально) Выделение серии VLAN или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Выделение диапазона VLAN. Пробелы до и после дефиса недопустимы.
<b>static</b>	(Опционально) Укажите при необходимости отбрасывать пакет, если пара привязки IP-to-Ethernet MAC не разрешена ARP ACL.

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

Данная команда используется для указания списка доступа ARP, который будет использоваться для проверки ARP Inspection для VLAN. Для одной VLAN можно указать один список доступа.

Dynamic ARP Inspection проверяет ARP-пакеты, полученные в VLAN, для проверки корректности пары привязки IP-адреса источника и MAC-адреса источника. Во время проверки произойдет сопоставление адреса привязки и записей из таблицы привязки DHCP Snooping. Проверка будет производиться, если данная команда сконфигурирована.

Списки управления доступом ARP (ARP ACL) имеют более высокий приоритет над таблицей привязки DHCP Snooping. Если пакету явно запрещен доступ списком управления доступом, пакет будет отброшен. Если пакету неявно запрещен доступ, он будет дополнительно сопоставлен с записями привязки DHCP Snooping, если не указано ключевое слово **«static»**. Если пакету неявно запрещен доступ и указано ключевое слово **«static»**, пакет будет отброшен.

### Пример

В данном примере показано, как применить список управления доступом ARP (ARP ACL) static ARP list в VLAN 10 для DAI.

```
Switch# configure terminal
Switch(config)# ip arp inspection filter static-arp-list vlan 10
Switch(config)#
```

## 23-5 ip arp inspection limit

Данная команда используется для ограничения скорости входящих ARP-запросов и ответов на интерфейсе. При использовании формы **no** команда вернется к значениям по умолчанию.

```
ip arp inspection limit {rate VALUE [burst interval SECONDS] | none}
no ip arp inspection limit
```

### Параметры

<b>rate VALUE</b>	Укажите максимальное количество ARP-пакетов в секунду, которое может быть обработано. Доступен диапазон значений от 1 до 150.
<b>burst interval SECONDS</b>	(Опционально) Укажите разрешенную величину продолжительности всплеска (burst duration) ARP-пакетов. Доступен диапазон значений от 1 до 15. Если не указано, значение по умолчанию составляет 1 секунду.
<b>none</b>	Укажите, чтобы скорость передачи ARP-пакетов не была ограничена.

### По умолчанию

Для недоверенных интерфейсов DAI ограничение скорости составляет 15 пакетов в секунду интервалом всплеска burst interval в 1 секунду.

Для доверенных интерфейсов DAI ограничений нет.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Данная команда используется и для доверенных, и для недоверенных интерфейсов. Если скорость ARP-пакетов в секунду превышает ограничение и условия для настроенной продолжительности всплеска (burst duration), порт автоматически отключится из-за ошибки.

### Пример

В данном примере показано, как назначить ограничение скорости входящих ARP-запросов до 30 пакетов в секунду и интервал проверки интерфейса до 5 следующих секунд.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/10
Switch(config-if)# ip arp inspection limit rate 30 burst interval 5
Switch(config-if)#
```

## 23-6 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

<i>NUMBER</i>	Укажите количество записей в буфере. Максимальное значение – 1024.
---------------	--

#### По умолчанию

Значение по умолчанию – 32.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Данная команда используется для настройки максимального количества записей в буфере журнала. Буфер журнала ARP Inspection хранит информацию об ARP-пакетах. Первый пакет, прошедший через проверку, будет отправлен в модуль системного журнала (syslog) и записан в буфер журнала проверки. Последующие пакеты из той же сессии не будут отправлены в модуль журнала, если только его запись в буфере журнала не будет удалена. Если буфер журнала полон, но события продолжают поступать, они не будут записаны в журнал. Если пользователь задает размер буфера меньше текущего номера записи, буфер журнала (лога) будет очищен автоматически.

#### Пример

В данном примере показано, как изменить размер буфера на 64.

```
Switch# configure terminal
Switch(config)# ip arp inspection log-buffer entries 64
Switch(config)#
```

## 23-7 ip arp inspection trust

Данная команда используется для назначения доверенного интерфейса для Dynamic ARP Inspection. При использовании формы **no** команда отключит режим доверенного интерфейса.

```
ip arp inspection trust
no ip arp inspection trust
```

#### Параметры

Нет

#### По умолчанию

По умолчанию данная опция отключена.

#### Режим ввода команды



## Interface Configuration Mode

**Использование команды**

Если интерфейс находится в состоянии Trust (доверенный), ARP-пакеты, поступающие на интерфейс, не будут проверяться. Если интерфейс находится в состоянии Untrusted (недоверенный), ARP-пакеты, поступающие на порт и принадлежащие VLAN, в которой включена проверка, будут проверяться.

**Пример**

В данном примере показано, как настроить состояние Trust (доверенный) для порта 1/0/3 для DAI.

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

**23-8 ip arp inspection validate**

Данная команда используется для указания дополнительных проверок при ARP Inspection. При использовании формы **no** команда отключит дополнительные проверки.

**ip arp inspection validate [src-mac] [dst-mac] [ip]**  
**no ip arp inspection validate [src-mac] [dst-mac] [ip]**

**Параметры**

<b>src-mac</b>	(Опционально) Укажите для проверки пакетов ARP-запросов и ответов, а также согласованности MAC-адреса источника в заголовке Ethernet с MAC-адресом источника в ARP заголовке.
<b>dst-mac</b>	(Опционально) Укажите для проверки пакетов ARP-ответов, а также согласованности MAC-адреса источника в заголовке Ethernet с MAC-адресом источника в ARP заголовке.
<b>ip</b>	(Опционально) Укажите для проверки содержимого ARP на наличие недопустимых и непредвиденных IP-адресов. Укажите для проверки допустимости IP-адреса в заголовке ARP. Проверяются IP-адреса источника во всех ARP-запросах и ответах, а также IP-адрес назначения в ARP-ответе. Пакеты, отправляемые на IP-адреса 0.0.0.0, 255.255.255.255 и все IP-адреса многоадресной рассылки, отбрасываются. IP-адреса источника проверяются во всех ARP-запросах и ответах, а IP-адреса назначения проверяются только в ARP-ответах.

**По умолчанию**

По умолчанию данная опция отключена.

**Режим ввода команды**

Global Configuration Mode

## Использование команды

Данная команда используется для указания дополнительных проверок во время Dynamic ARP Inspection. Указанные проверки будут производиться с пакетами, присылаемыми с недоверенных интерфейсов и принадлежащих VLAN, для которых включена IP ARP Inspection. Если никакие параметры не указаны, все опции включены или выключены. При использовании формы `no` команда отключит дополнительные типы проверок.

## Пример

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

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

## 23-9 ip arp inspection vlan

Данная команда используется для включения Dynamic ARP Inspection для определенных VLAN. При использовании формы `no` команда отключит Dynamic ARP Inspection для VLAN.

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

## Параметры

<b>vlan</b> <i>VLAN-ID</i>	Укажите VLAN, для которой необходимо включить или отключить функцию ARPInspection.
,	(Опционально) Выделение серии или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон VLAN. Пробелы до и после дефиса недопустимы.

## По умолчанию

По умолчанию ARP Inspection отключена для всех VLAN.

## Режим ввода команды

Global Configuration Mode

## Использование команды

Когда VLAN включена для проверки ARP, ARP-пакеты, включая как ARP-запрос, так и ответный пакет, принадлежащие VLAN, поступающие на недоверенный интерфейс, будут проверяться. Если пара связывания IP-MAC адресов MAC-адреса источника и IP-адреса источника не разрешена ARP ACL или базой данных связывания DHCP snooping, ARP-пакет будет отброшен. В дополнение к проверке привязки адресов будет также проверена дополнительная проверка, определенная командой проверки IP ARP inspection validate.

## Пример

В данном примере показано, как включить ARP Inspection в VLAN 2.

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 2
Switch(config)#
```

## 23-10 ip arp inspection vlan logging

Данная команда используется для управления типом пакетов, которые будут регистрироваться (логироваться). При использовании формы **no** команда вернется к значениям по умолчанию.

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

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

### Параметры

<i>VLAN-ID</i>	Укажите VLAN, для которой необходимо включить или отключить функцию управления логированием.
,	(Опционально) Выделение серии или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон VLAN. Пробелы до и после дефиса недопустимы.
<b>acl-match</b>	Укажите критерии логирования для пакетов, отброшенных или разрешенных на основе совпадения со списком управления доступом (ACL).
<b>permit</b>	Укажите для логирования, разрешенного сконфигурированным списком управления доступом (ACL).
<b>all</b>	Укажите для логирования, разрешенного или запрещенного сконфигурированным списком управления доступом (ACL).
<b>none</b>	Укажите, чтобы отменить логирование пакетов на основе совпадения со списком управления доступом (ACL).
<b>dhcp-bindings</b>	Укажите критерии логирования для пакетов, отброшенных или разрешенных на основе совпадения с привязкой DHCP.
<b>permit</b>	Укажите для логирования, разрешенного привязкой DHCP.
<b>all</b>	Укажите для логирования, разрешенного или запрещенного привязкой DHCP.
<b>none</b>	Укажите, чтобы отменить логирование всех пакетов, разрешенных или запрещенных на основе привязки DHCP.

### По умолчанию

Все отклоненные или отброшенные пакеты регистрируются в журнале.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте форму **no**, чтобы команда вернулась к критериям логирования по умолчанию.

### Пример

В этом примере показано, как настроить проверку ARP на VLAN 1 для добавления в журнал пакетов, соответствующих ACL.

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

## 23-11 permit | deny (arp access-list)

Данная команда используется для управления доступом ARP-записи. Используйте команду **deny** для создания запрещающей ARP-записи. При использовании формы **no** команда удалит запись.

```
{permit | deny} ip {any | host SENDER-IP | SENDER-IP SENDER-IP-MASK} mac {any | host SENDER-MAC |
SENDER-MAC SENDER-MAC-MASK}
no {permit | deny} ip {any | host SENDER-IP | SENDER-IP SENDER-IP-MASK} mac {any | host SENDER-
MAC | SENDER-MAC SENDER-MAC-MASK}
```

### Параметры

<b>ip</b>	Укажите IP-адрес источника.
<b>any</b>	Укажите для сопоставления любого IP-адреса источника.
<b>host SENDER-IP</b>	Укажите для сопоставления единственного IP-адреса источника.
<i>SENDER-IP SENDER-IP-MASK</i>	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.
<b>mac</b>	Укажите MAC-адрес.
<b>any</b>	Укажите для сопоставления любого MAC-адреса источника.
<b>host SENDER-MAC</b>	Укажите для сопоставления единственного MAC-адреса источника.
<i>SENDER-MAC SENDER-MAC-MASK</i>	Укажите для сопоставления группы MAC-адресов источника с помощью битовой маски (bitmap). Проверяться будет бит, соответствующий значению бита 1. Формат ввода тот же, что и для MAC-адреса.

### По умолчанию

Нет

### Режим ввода команды

ARP Access-list Configuration Mode

### Использование команды

Используйте опцию **permit any**, чтобы команда разрешила доступ остальным пакетам, не прошедшим проверку по предыдущим правилам.

## Пример

В этом 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)#
```

## 23-12 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

<b>interface</b> <i>INTERFACE-ID</i>	(Опционально) Интерфейс (порт), группа интерфейсов (портов) или все интерфейсы (порты), которые необходимо настроить
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Выделение диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
<b>statistics</b>	(Опционально) Указывает данные статистики DAI.
<b>vlan</b> <i>VLAN-ID</i>	(Опционально) Укажите VLAN или группу VLAN.
,	(Опционально) Выделение серии VLAN или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Выделение диапазона VLAN. Пробелы до и после дефиса недопустимы.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Данная команда используется для отображения статуса DAI для указанного диапазона VLAN.

## Пример

В данном примере показано, как включить отображение параметров статистики пакетов, которые были обработаны DAI для VLAN 10.

```
Switch# show ip arp inspection statistics vlan 10

VLAN    Forwarded    Dropped    DHCP Drops    ACL Drops
-----
10      21546        145261     145261        0
VLAN    DHCP Permits  ACL Permits  Source MAC Failures
-----
10      21546         0           0
VLAN    Dest MAC Failures  IP Validation Failures
-----
10      0                0

Switch#
```

В данном примере показано, как включить отображение параметров статистики пакетов, которые были обработаны DAI для всех активных VLAN.

```
Switch# show ip arp inspection statistics

VLAN    Forwarded    Dropped    DHCP Drops    ACL Drops
-----
1       0            0           0             0
2       0            0           0             0
10      21546        145261     145261        0
100     0            0           0             0
200     0            0           0             0
1024    0            0           0             0
VLAN    DHCP Permits  ACL Permits  Source MAC Failures
-----
1       0            0           0
2       0            0           0
10      21546         0           0
100     0            0           0
200     0            0           0
1024    0            0           0
VLAN    Dest MAC Failures  IP Validation Failures
-----
1       0                   0
2       0                   0
10      0                   0
100     0                   0
200     0                   0
1024    0                   0

Switch#
```

#### Отображаемые параметры

<b>VLAN</b>	VLAN ID, на которой действует ARP Inspection.
<b>Forwarded</b>	Количество ARP-пакетов, переадресованных ARP Inspection.

<b>Dropped</b>	Количество ARP-пакетов, отброшенных ARP Inspection.
<b>DHCP Drops</b>	Количество ARP-пакетов, отброшенных таблицей DHCP Snooping.
<b>ACL Drops</b>	Количество ARP-пакетов, отброшенных с помощью ARP правил ACL (ARP ACL).
<b>DHCP Permits</b>	Количество ARP-пакетов, разрешенных таблицей привязки DHCP Snooping.
<b>ACL Permits</b>	Количество ARP-пакетов, разрешенных правилом ARP ACL.
<b>Source MAC Failures</b>	Количество ARP-пакетов, не прошедших проверку MAC-адреса источника.
<b>Dest MAC Failures</b>	Количество ARP-пакетов, не прошедших проверку MAC-адреса назначения.
<b>IP Validation Failures</b>	Количество ARP-пакетов, не прошедших проверку IP-адреса.

### Пример

В данном примере показано, как включить отображение настроек и статус работы DAI.

```
Switch#show ip arp inspection

Source MAC Validation      : Disabled
Destination MAC Validation: Disabled
IP Address Validation     : Disabled
VLAN State      ACL Match      Static ACL
-----
2      Enabled  -              -
VLAN ACL Logging DHCP Logging
-----
2      None      None

Switch#
```

### Отображаемые параметры

<b>VLAN</b>	VLAN ID, на которой действует ARP Inspection.
<b>State</b>	Состояние настроек ARP Inspection. <b>Enabled:</b> ARP Inspection работает. <b>Disabled:</b> ARP Inspection не работает.
<b>ACL Match</b>	Имя указанного списка управления доступом ARP (ARP ACL).
<b>Static ACL</b>	Настройки статического списка управления доступом (static ACL). <b>Yes:</b> статический список управления доступом (static ARP ACL) настроен. <b>No:</b> статический список управления доступом (static ARP ACL) не настроен.
<b>ACL logging</b>	Состояние логирования для пакетов, отброшенных или

---

разрешенных на основесовпадения со списком управления доступом (ACL).

**None:** пакеты, разрешенные списком управления доступом (ACL), не логируются.

**Permit:** логирование происходит, если пакеты разрешены настроенным списком управления доступом (ACL).

**Deny:** логирование происходит, если пакеты отброшены настроенным списком управления доступом (ACL).

**All:** логирование для всех пакетов, разрешенных настроенным списком управления доступом (ACL).

---

#### DHCP Logging

Состояние логирования для пакетов, отброшенных или разрешенных на основетаблицы привязки DHCP.

**None:** пакеты, отброшенные или разрешенные таблицей привязки DHCP, не логируются.

**Permit:** логирование происходит, если пакеты разрешены таблицей привязки DHCP.

**Deny:** логирование происходит, если пакеты отброшены таблицей привязки DHCP.

**All:** пакеты, отброшенные или разрешенные таблицей привязки DHCP, логируются.

---

В этом примере показано, как отобразить состояние доверия для интерфейса eth3/0/3.

```
Switch#show ip arp inspection interfaces eth1/0/3

Interface      Trust State Rate(pps) Burst Interval
-----
eth1/0/3       untrusted  15         1
Total Entries: 1

Switch#
```

В данном примере показано, как включить отображение состояний для интерфейсов коммутатора.



```
Switch#show ip arp inspection interfaces eth1/0/1-7
```

```

Interface          Trust State Rate(pps)  Burst Interval
-----
eth1/0/1           untrusted  15         1
eth1/0/2           untrusted  15         1
eth1/0/3           untrusted  15         1
eth1/0/4           untrusted  15         1
eth1/0/5           untrusted  15         1
eth1/0/6           untrusted  15         1
eth1/0/7           untrusted  15         1
Total Entries: 7

Switch#
```

#### Отображаемые параметры

<b>Interface</b>	Имя интерфейса, на котором работает ARP Inspection.
<b>Trust State</b>	Состояние интерфейса. <b>trusted:</b> данный интерфейс является доверенным портом ARP Inspection, все ARP-пакеты будут достоверны, и не будут проходить авторизацию. <b>untrusted:</b> данный интерфейс является недоверенным портом ARP Inspection, все ARP-пакеты будут проходить авторизацию.
<b>Rate (pps)</b>	Верхняя граница количества входящих пакетов, обрабатываемых в секунду.
<b>Burst Interval</b>	Последовательный интервал в секундах, в течение которого на интерфейсе анализируется частота появления ARP-трафика.

## 28-13 show ip arp inspection log

Данная команда используется для отображения буфера лога (журнала) ARP Inspection.

```
show ip arp inspection log
```

#### Параметры

Нет

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

**Использование команды**

Данная команда используется для отображения содержимого буфера лога (журнала) ARP Inspection.

**Пример**

В данном примере показано, как включить отображение буфера лога (журнала) ARP Inspection.

```
Switch# show ip arp inspection log

Total log buffer size: 64

Interface    VLAN      Sender IP      Sender MAC      Occurrence
-----
eth1/0/1     100       10.20.1.1      00-20-30-40-50-60  1 (2014-03-28 23:08:66)
eth1/0/2     100       10.5.10.16     55-66-20-30-40-50  2 (2014-04-02 00:11:54)
eth1/0/3     100       10.58.2.30     10-22-33-44-50-60  1 (2014-03-30 12:01:38)

Total Entries: 3

Switch#
```

**Отображаемые параметры**

<b>Interface</b>	Имя интерфейса, на котором производится логирование.
<b>VLAN</b>	VLAN, на которой производится логирование.
<b>Sender IP</b>	MAC-адрес источника у логируемого ARP.
<b>Occurence</b>	Счетчик общего числа логирования записей, а также времени последнего случившегося логирования.

## 24. Команды Error Recovery

### 24-1 errdisable recovery

Данная команда используется для включения функции Error Recovery (восстановление ошибок), а также для настройки Recovery Interval (время восстановления). Используйте форму **no**, чтобы отключить опцию Auto-Recovery или вернуться к настройкам по умолчанию.

**errdisable recovery cause {all | psecure-violation | storm-control | bpdu-protect | arp-rate | dhcp-rate | loopback-detect} [interval SECONDS]**

**no errdisable recovery cause {all | psecure-violation | storm-control | bpdu-protect | arp-rate | dhcp-rate | loopback-detect | l2pt-guard | duld} [interval SECONDS]**

#### Параметры

<b>all</b>	Укажите, чтобы включить опцию Auto-Recovery для всех ситуаций.
<b>psecure-violation</b>	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной Port Security Violation.
<b>storm-control</b>	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной Storm Control.
<b>bpdu-protect</b>	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной BPDU Protection.
<b>arp-rate</b>	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной ARP Rate Limiting.
<b>dhcp-rate</b>	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной DHCP Rate Limiting.
<b>loopback-detect</b>	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной Loop Detection.
<b>interval SECONDS</b>	Укажите время, необходимое для восстановления порта при ошибке, вызванной указанным модулем. Доступный диапазон значений: от 5 до 86400 секунд. Значение по умолчанию – 300 секунд.

#### По умолчанию

По умолчанию опция Auto-Recovery отключена для всех ситуаций.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Ошибка на порту может быть вызвана Port Security Violations, Storm Control и так далее. При возникновении ошибки порт отключается, однако для настроек конфигурации будет действовать опция **no shutdown**.

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

### Пример

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

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

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

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

## 24-2 show errdisable recovery

Данная команда используется для отображения настроек Recovery Timer (таймер восстановления).

**show errdisable recovery**

### Параметры

Нет

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте данную команду, чтобы отобразить настройки Recovery Timer.

### Пример

В данном примере показано, как отобразить настройки Recovery Timer.

```
Switch#show errdisable recovery
```

ErrDisable Cause	State	Interval
Port Security	enabled	200 seconds
Storm Control	disabled	300 seconds
BPDU Attack Protection	disabled	300 seconds
Dynamic ARP Inspection	disabled	300 seconds
DHCP Snooping	disabled	300 seconds
Loop Detection	disabled	300 seconds

```
Interfaces that will be recovered at the next timeout:
```

```
Switch#
```

### 24-3 snmp-server enable traps errdisable

Эта команда используется для включения отправки SNMP-уведомлений для отключенного состояния ошибки. Используйте форму **no** этой команды, чтобы отключить отработку SNMP-уведомлений.

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

#### Параметры

<b>asserted</b>	(Опционально) Укажите, чтобы включить/отключить отработку SNMP-уведомлений об ошибке на порту.
<b>cleared</b>	(Опционально) Укажите, чтобы включить/отключить отработку SNMP-уведомлений об устранении ошибки.
<b>notification-rate TRAP-RATE</b>	(Опционально) Укажите количество трапов в минуту. Доступный диапазон значений: от 0 до 1000. Если количество пакетов превысило указанное значение, все последующие пакеты будут отброшены. Если указан 0, ограничения по количеству отсылаемых SNMP-уведомлений об ошибке в минуту отсутствуют.

#### По умолчанию

По умолчанию данная опция отключена.  
 Количество уведомлений в минуту по умолчанию – 0.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Эта команда с параметрами **asserted** и **cleared** включает или отключает уведомления об изменении состояния error disabled. Если вы вводите команду с одним из параметров, включается или отключается только указанный тип уведомления. Состояние или значение другого типа уведомлений не затрагивается.

Команды **snmp-server enable traps errdisable notification-rate** и **no snmp-server enable traps errdisable notification-rate** влияют только на настройку notification-rate, но не на состояние отправки уведомлений для состояния error disabled.

#### Пример

В этом примере показано, как включить отправку ловушек для входа в состояние error disabled и выхода из него и установить максимальное количество ловушек в секунду равным 3.

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

## 25. Команды File System

### 25-1 delete

Данная команда используется для удаления файла.

**delete** *FILE-URL*

#### Параметры

<i>FILE-URL</i>	Укажите имя файла, который необходимо удалить.
-----------------	--

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Образ прошивки или файл конфигурации, указанный в качестве загрузочного файла, не может быть удален.

#### Пример

В этом примере показано, как удалить файл с именем "Image2" из файловой системы на локальной флэш-памяти.

```
Switch#delete Image2
Delete Image2? (y/n) [n]  y
File is deleted.

Switch#
```

### 25-2 dir

Данная команда используется для отображения информации о файле или списке файлов в указанном пути.

**dir** [*URL*]

#### Параметры

<i>URL</i>	(Опционально) Укажите имя файла или каталога, который необходимо отобразить.
------------	--

#### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Если параметр не указан, используется текущий каталог. По умолчанию текущий непосредственно находится в корне файловой системы, расположенной на локальной флэш-памяти. Носитель информации монтируется в файловую систему и отображается пользователю как подкаталог под корневым каталогом.

Поддерживаемые файловые системы могут быть отображены при выполнении пользователем команды `dir` для корневого каталога. Носитель информации, сопоставленный с файловой системой, можно отобразить с помощью команды `show storage media`.

### Пример

В этом примере показано, как отобразить каталог `root` в автономном коммутаторе.

```
Switch#dir
Directory of /c:
1  -rw          1062 Sep 24 2019 01:28:50  512_SSL_certificate.crt
2  -rw           887 Sep 24 2019 01:29:40  512_SSL-private.prv
3  -rw      8486640 Sep 23 2019 02:16:36  Image1
4  -rw      8485024 Sep 16 2019 02:47:21  Image2
5  -rw      160223 Sep 20 2019 03:33:54  Config1
6  -rw       1338 Sep 24 2019 01:30:06  512_SSL_CertificateAuthority.ca
7  d--       1360 Jan 01 2000 00:00:08  system

46305280 bytes total (20725760 bytes free)

Switch#
```

## 25-3 show storage media-info

Данная команда используется для отображения информации о накопителе.

### show storage media-info

#### Параметры

Нет

#### По умолчанию

Нет

#### Режим ввода команды



EXEC Mode

### Использование команды

Используйте эту команду для отображения информации о носителях информации, доступных в системе.

### Пример

В данном примере показано, как отобразить информацию о носителе информации.

```
Switch#show storage media-info

Drive  Media Type  Size      FS-Type  Label
-----  -
c:     Flash        44 MB    swfs

Switch#
```

## 26. Команды Filter Database (FDB)

### 26-1 clear mac-address-table

Данная команда используется для удаления указанного динамического MAC-адреса, всех динамических MAC-адресов на указанном интерфейсе, всех динамических MAC-адресов на указанной VLAN или всех динамических MAC-адресов из таблицы MAC-адресов.

```
clear mac-address-table dynamic {all | address MAC-ADDR | interface INTERFACE-ID | vlan VLAN-ID}
```

#### Параметры

<b>all</b>	Укажите, чтобы удалить все динамические MAC-адреса.
<b>address</b> <i>MAC-ADDR</i>	Укажите, чтобы удалить указанный динамический MAC-адрес.
<b>interface</b> <i>INTERFACE-ID</i>	Укажите интерфейс (физический порт или port-channel), на котором необходимо удалить MAC-адрес.
<b>vlan</b> <i>VLAN-ID</i>	Укажите VLAN ID в диапазоне от 1 до 4094.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте данную команду, чтобы удалить записи динамических MAC-адресов. Будет удален только динамический индивидуальный адрес.

#### Пример

В данном примере показано, как удалить MAC-адрес 00:08:00:70:00:07 из таблицы динамических MAC-адресов.

```
Switch# clear mac-address-table dynamic address 00:08:00:70:00:07
Switch#
```

### 26-2 mac-address-table aging-time

Данная команда используется для настройки времени устаревания MAC-адресов в таблице. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
mac-address-table aging-time SECONDS
no mac-address-table aging-time
```

#### Параметры

<i>SECONDS</i>	Укажите время устаревания в диапазоне от 0 или 10 до 1000000 секунд. Укажите 0, чтобы отключить функцию устаревания MAC-адресов в таблице.
----------------	--

**По умолчанию**

Значение по умолчанию – 300 секунд.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Укажите время устаревания 0, чтобы отключить функцию устаревания MAC-адресов в таблице.

**Пример**

В данном примере показано, как установить значение времени устаревания на 200 секунд.

```
Switch# configure terminal
Switch(config)# mac-address-table aging-time 200
Switch(config)#
```

**26-3 mac-address-table learning**

Эта команда используется для включения обучения MAC-адресов на физическом порту. Используйте форму **no** этой команды, чтобы отключить обучение.

**mac-address-table learning interface {*INTERFACE-ID* [, | -]}**  
**no mac-address-table learning interface {vlan *VLAN-ID* [, | -] | *INTERFACE-ID* [, | -]}**

**Параметры**

<i>INTERFACE-ID</i>	Укажите интерфейс физического порта, который необходимо сконфигурировать.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

**По умолчанию**

По умолчанию данная опция включена.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Используйте эту команду для включения или отключения обучения MAC-адресов на физическом порту.

### Пример

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

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

## 26-4 mac-address-table notification change

Данная команда используется для включения/настройки функции уведомлений о MAC-адресах. Используйте форму **no**, чтобы отключить функцию или вернуться к настройкам по умолчанию.

**mac-address-table notification change [interval SECONDS | history-size VALUE | trap-type {with-vlanid | without-vlanid}]**  
**no mac-address-table notification change [interval | history-size | trap-type]**

### Параметры

<b>interval SECONDS</b>	(Опционально) Укажите интервал отправки трап-сообщений о MAC-адресах в диапазоне от 1 до 2147483647 секунд. Значение по умолчанию – 1 секунда.
<b>history-size VALUE</b>	(Опционально) Укажите максимальное количество записей в таблице истории уведомлений. Доступный диапазон значений: от 0 до 500 записей. Значение по умолчанию – 1 запись.
<b>trap-type</b>	(Опционально) Указывает, включать или нет идентификатор виртуальной локальной сети в информацию о ловушке.
<b>with-vlanid</b>	Указывает информацию о трапа для включения идентификатора виртуальной локальной сети.
<b>without-vlanid</b>	Указывает информацию трапа для исключения идентификатора VLAN.

### По умолчанию

Уведомление о MAC-адресе отключено.

Интервал срабатывания ловушки по умолчанию составляет 1 секунду.

Число записей в таблице истории по умолчанию равно 1.

Тип ловушки по умолчанию - **without-vlanid**.

### Режим ввода команды

Global Configuration Mode

### Использование команды

При распознавании или удалении коммутатором MAC-адреса соответствующее уведомление может быть отправлено в таблицу истории уведомлений, а затем на SNMP-сервер, если запущена команда **snmp-server enable traps mac-notification change**. В таблице истории уведомлений хранятся распознанные или

удаленные MAC-адреса тех интерфейсов, для которых включены трапы. Для групповых адресов события не генерируются.

### Пример

В данном примере показано, как включить уведомления об изменении MAC-адреса и установить интервал 10 секунд, а лимит по количеству записей в истории – 500.

```
Switch# configure terminal
Switch(config)# mac-address-table notification change
Switch(config)# mac-address-table notification change interval 10
Switch(config)# mac-address-table notification change history-size 500
Switch(config)#
```

## 26-5 mac-address-table static

Данная команда используется для добавления статического адреса в таблицу MAC-адресов. Используйте форму **no**, чтобы удалить запись из таблицы.

**mac-address-table static** *MAC-ADDR* **vlan** *VLAN-ID* {**interface** *INTERFACE-ID* [, | -] | **drop**}  
**no mac-address-table static** {**all** | *MAC-ADDR* **vlan** *VLAN-ID* [**interface** *INTERFACE-ID*] [, | -]}

### Параметры

<i>MAC-ADDR</i>	Укажите индивидуальный или групповой MAC-адрес. Пакеты с адресом назначения (destination), соответствующим данному MAC-адресу, полученные указанной VLAN, будут направлены на указанный интерфейс.
<b>vlan</b> <i>VLAN-ID</i>	Укажите VLAN записи в диапазоне от 1 до 4094.
<b>interface</b> <i>INTERFACE-ID</i>	Укажите порты продвижения кадров.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
<b>drop</b>	Укажите, чтобы отбросить кадры, отправленные с указанного MAC-адреса / на указанный MAC-адрес на обозначенной VLAN.
<b>all</b>	Укажите, чтобы удалить все записи статических MAC-адресов.

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

Для записи индивидуального MAC-адреса можно указать только один интерфейс. Для записи группового MAC-адреса можно указать несколько интерфейсов. Чтобы удалить запись индивидуального MAC-адреса, interface ID указывать не нужно. При удалении записи группового MAC-адреса будет удален только тот интерфейс, ID которого указан. Если interface ID не указан, будет удалена вся запись группового MAC-адреса. Параметр drop может быть применен только для записи индивидуального MAC-адреса.

### Пример

В этом примере показано, как добавить статический адрес C2:F3:22:0A:12:F4 в таблицу MAC-адресов. Он также указывает, что при получении любого пакета в сети VLAN 4, имеющего MAC-адрес назначения C2:F3:22:0A:12:F4, он будет перенаправлен на порт 1.

```
Switch# configure terminal
Switch(config)# mac-address-table static C2:F3:22:0A:12:F4 vlan 4 interface
eth1/0/1
Switch(config)#
```

## 26-6 multicast filtering-mode

Данная команда используется для настройки способа обработки групповых пакетов на интерфейсе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**multicast filtering-mode {forward-all | forward-unregistered | filter-unregistered}**  
**no multicast filtering-mode**

### Параметры

<b>forward-all</b>	Задает рассылку всех многоадресных пакетов на основе домена VLAN.
<b>forward-unregistered</b>	Определяет пересылку зарегистрированных многоадресных пакетов на основе таблицы пересылки и пересылку всех незарегистрированных многоадресных пакетов на основе домена VLAN.
<b>filter-unregistered</b>	Указывает пересылать зарегистрированные пакеты на основе таблицы пересылки и фильтровать все незарегистрированные многоадресные пакеты.

### По умолчанию

По умолчанию опция **forward-unregistered** включена.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Данный режим фильтрации применим только к групповым пакетам, предназначенным для адресов, незарезервированных для групповых адресов.

### Пример

В данном примере показано, как установить режим фильтрации групповых пакетов на VLAN 100, чтобы отфильтровать незарегистрированные адреса.

```
Switch# configure terminal
Switch(config)# vlan 100
Switch(config-vlan)# multicast filtering-mode filter-unregistered
Switch(config-vlan)#
```

## 26-7 show mac-address-table

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

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

### Параметры

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

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

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

### Пример

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

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

VLAN	MAC Address	Type	Ports
1	00-02-4B-28-C4-82	Static	CPU

```
Total Entries: 1

Switch#
```

В данном примере показано, как отобразить все записи таблицы статических MAC-адресов.

```
Switch# show mac-address-table static
```

VLAN	MAC Address	Type	Ports
1	00-02-4B-28-C4-82	Static	CPU
2	00-02-4B-28-C4-82	Static	CPU
4	00-01-00-02-00-04	Static	eth1/0/2
4	C2-F3-22-0A-12-F4	Static	port-channel2
6	00-01-00-02-00-07	Static	eth1/0/1
6	00-01-00-02-00-10	Static	Drop

```
Total Entries : 6

Switch#
```

В данном примере показано, как отобразить все записи таблицы MAC-адресов для VLAN 1.

```
Switch# show mac-address-table vlan 1
```

VLAN	MAC Address	Type	Ports
1	00-02-4B-28-C4-82	Static	CPU
1	00-03-40-11-22-33	Dynamic	eth1/0/2

```
Total Entries: 2

Switch#
```

## 26-8 show mac-address-table aging-time

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

**show mac-address-table aging-time**

**Параметры**



Нет

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте данную команду, чтобы отобразить время устаревания MAC-адресов в таблице.

**Пример**

В данном примере показано, как отобразить время устаревания MAC-адресов в таблице.

```
Switch# show mac-address-table aging-time
Aging Time is 300 seconds
Switch#
```

**26-9 show mac-address-table learning**

Данная команда используется для отображения статуса изучения MAC-адресов.

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

**Параметры**

<i>INTERFACE-ID</i>	(Опционально) Укажите интерфейс, который необходимо отобразить.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Если не указаны дополнительные параметры, будут отображены все физические порты.

### Пример

В данном примере показано, как отобразить статус изучения MAC-адресов на всех физических портах от 1 до 10.

```
Switch#show mac-address-table learning interface ethernet 1/0/1-10

Port                State
-----
eth1/0/1            Enabled
eth1/0/2            Enabled
eth1/0/3            Enabled
eth1/0/4            Enabled
eth1/0/5            Enabled
eth1/0/6            Enabled
eth1/0/7            Enabled
eth1/0/8            Enabled
eth1/0/9            Enabled
eth1/0/10           Enabled

Switch#
```

## 26-10 show mac-address-table notification change

Данная команда используется для отображения настроек уведомлений о MAC-адресах или истории уведомлений.

**show mac-address-table notification change [interface [INTERFACE-ID] | history]**

### Параметры

<b>interface</b> INTERFACE-ID	(Опционально) Укажите интерфейс, который необходимо отобразить.
<b>history</b>	(Опционально) Укажите, чтобы отобразить историю уведомлений об изменении MAC-адреса.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Если параметр не указан, будет отображена глобальная конфигурация. Используйте параметр **interface** для отображения информации обо всех интерфейсах. Используйте параметр **interface INTERFACE-ID** для отображения информации об указанном интерфейсе.

**Пример**

В данном примере показано, как отобразить настройки уведомлений об изменении MAC-адреса на всех интерфейсах.

```
Switch#show mac-address-table notification change interface
```

Interface	Added Trap	Removed Trap
-----	-----	-----
eth1/0/1	Disabled	Disabled
eth1/0/2	Disabled	Disabled
eth1/0/3	Disabled	Disabled
eth1/0/4	Disabled	Disabled
eth1/0/5	Disabled	Disabled
eth1/0/6	Disabled	Disabled
eth1/0/7	Disabled	Disabled
eth1/0/8	Disabled	Disabled
eth1/0/9	Disabled	Disabled
eth1/0/10	Disabled	Disabled
eth1/0/11	Disabled	Disabled
eth1/0/12	Disabled	Disabled
eth1/0/13	Disabled	Disabled
eth1/0/14	Disabled	Disabled
eth1/0/15	Disabled	Disabled
eth1/0/16	Disabled	Disabled
eth1/0/17	Disabled	Disabled
eth1/0/18	Disabled	Disabled
eth1/0/19	Disabled	Disabled
eth1/0/20	Disabled	Disabled
eth1/0/21	Disabled	Disabled
eth1/0/22	Disabled	Disabled
eth1/0/23	Disabled	Disabled
eth1/0/24	Disabled	Disabled
eth1/0/25	Disabled	Disabled
eth1/0/26	Disabled	Disabled
eth1/0/27	Disabled	Disabled
eth1/0/28	Disabled	Disabled
Switch#		

В данном примере показано, как отобразить общие настройки уведомлений о MAC-адресах.

```
Switch#show mac-address-table notification change

MAC Notification Change Feature: Disabled
Interval between Notification Traps: 1 seconds
Maximum Number of Entries Configured in History Table: 1
Current History Table Length: 0
MAC Notification Trap State: Disabled

Switch#
```

В данном примере показано, как отобразить историю уведомлений о MAC-адресах.

```
Switch# show mac-address-table notification change history

History Index: 1
Operation:ADD Vlan: 1 MAC Address: 00-f8-d0-12-34-56 eth1/0/1
History Index: 2
Operation:DEL Vlan: 1 MAC Address: 00-f8-d0-00-00-01 eth1/0/1
History Index: 3
Operation:DEL Vlan: 1 MAC Address: 00-f8-d0-00-00-02 eth1/0/1

Switch#
```

## 26-11 show multicast filtering-mode

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

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

### Параметры

---

<b>interface</b> <i>INTERFACE-ID</i>	(Опционально) Укажите VLAN, которую необходимо отобразить.
--------------------------------------	--

---

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте эту команду для отображения режима фильтрации для обработки многоадресных пакетов, полученных на интерфейсе.

## Пример

В данном примере показано, как отобразить настройки режима фильтрации групповых пакетов для всех VLAN.

```
Switch#show multicast filtering-mode

Interface                               Layer 2 Multicast Filtering Mode
-----                               -
default                                 forward-unregistered

Total Entries: 1

Switch#
```

## 26-12 snmp-server enable traps mac-notification change

Данная команда используется для включения отправки SNMP Trap об уведомлениях MAC. Используйте форму **no**, чтобы отключить данную функцию.

```
snmp-server enable traps mac-notification change
no snmp-server enable traps mac-notification change
```

### Параметры

Нет

### По умолчанию

По умолчанию данная опция отключена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду, чтобы включить отработку SNMP Trap об уведомлениях MAC.

## Пример

В данном примере показано, как включить отработку SNMP Trap об уведомлениях MAC.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps mac-notification change
Switch(config)#
```

## 26-13 snmp trap mac-notification change

Данная команда используется для включения уведомлений об изменении MAC-адреса на указанном интерфейсе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**snmp trap mac-notification change {added | removed}**  
**no snmp trap mac-notification change {added | removed}**

### Параметры

<b>added</b>	Укажите, чтобы включить уведомления об изменении MAC-адреса при добавлении MAC-адреса на интерфейс.
<b>removed</b>	Укажите, чтобы включить уведомления об изменении MAC-адреса при удалении MAC-адреса с интерфейса.

### По умолчанию

По умолчанию эта опция отключена.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Даже если при помощи команды **snmp trap mac-notification change** на интерфейсе включена отправка уведомлений, уведомления будут отправлены в таблицу истории только при использовании команды **mac-address-table notification change**.

### Пример

В данном примере показано, как включить уведомления о добавлении MAC-адреса на интерфейсе Ethernet 1/0/2.

```
Switch# configure terminal
Switch(config)# interface eth1/0/2
Switch(config-if)# snmp trap mac-notification change added
Switch(config-if)#
```

## 27. Команды Gratuitous ARP

### 27-1 snmp-server enable traps gratuitous-arp

Данная команда используется для включения отправки SNMP-уведомлений об обнаружении дублированного IP-адреса Gratuitous ARP. Используйте форму **no**, чтобы отключить данную функцию.

```
snmp-server enable traps gratuitous-arp  
no snmp-server enable traps gratuitous-arp
```

#### Параметры

Нет

#### По умолчанию

По умолчанию данная опция отключена.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Данная команда используется для включения/отключения отправки SNMP-уведомлений об обнаружении дублированного IP-адреса Gratuitous ARP.

#### Пример

В данном примере показано, как включить отставку SNMP-уведомлений об обнаружении дублированного IP-адреса Gratuitous ARP.

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

## 28. Команды управления интерфейсом

### 28-1 clear counters

Данная команда используется для сброса всех счетчиков для указанных интерфейсов.

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

#### Параметры

<b>all</b>	Укажите, если необходимо сбросить счетчики для всех интерфейсов.
<b>interface <i>INTERFACE-ID</i></b>	Указывает интерфейсы, которые необходимо очистить.
<b>,</b>	(Опционально) Указывает серию интерфейсов или отделяет диапазон интерфейсов от предыдущего диапазона. До или после запятой пробел не допускается.
<b>-</b>	(Опционально) Указывает диапазон интерфейсов. До или после дефиса пробел не допускается.

#### По умолчанию

Нет

#### Режим ввода команды

Privileged EXEC Mode

#### Использование команды

Команда используется для сброса счетчиков для интерфейса физического порта.

#### Пример

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

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

### 28-2 description

Данная команда используется для добавления описания для интерфейса. При использовании формы **no** команда удалит описание.

**description *STRING***  
**no description**

#### Параметры

<b><i>STRING</i></b>	Описание для интерфейса. Максимально допустимое количество символов – 64.
----------------------	---



**По умолчанию**

Нет

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Описание может быть добавлено к любому предварительно определенному типу интерфейса. Указанное описание соответствует объекту MIB "ifAlias", определенному в RFC 2233.

**Пример**

В данном примере показано, как добавить описание "Physical Port 10" к порту 10.

```
Switch# configure terminal
Switch(config)# interface eth1/0/10
Switch(config-if)# description Physical Port 10
Switch(config-if)#
```

В данном примере показано, как добавить описание "Data VLAN" к интерфейсу виртуальной локальной сети уровня 2.

```
Switch#configure terminal
Switch(config)#interface l2vlan 1
Switch(config-if)#description Data VLAN
Switch(config-if)#
```

**28-3 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**

<i>INTERFACE-ID</i>	Указывает идентификатор интерфейса. Идентификатор интерфейса формируется из типа интерфейса и номера интерфейса. Типы интерфейсов следующие: <ul style="list-style-type: none"> <li>- Ethernet - порт коммутатора Ethernet со всеми различными носителями.</li> <li>- Vlan - интерфейс VLAN.</li> <li>- Port-channel - интерфейс агрегированного портового канала.</li> <li>- range - Вход в режим конфигурации диапазона интерфейсов для нескольких интерфейсов.</li> </ul>
---------------------	--

---

- L2vlan - интерфейс виртуальной локальной сети второго уровня IEEE 802.1Q.

---

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

Эта команда входит в режим конфигурации интерфейса для конкретного интерфейса. Формат номера интерфейса зависит от типа интерфейса. Для интерфейсов физического порта пользователь не может войти в интерфейс, если порт коммутатора не существует. Интерфейс физического порта не может быть удален командой **no**.

Используйте команду **interface vlan** для создания интерфейсов уровня 3. Используйте команду **vlan** в режиме глобальной конфигурации для создания сети VLAN перед созданием интерфейсов уровня 3. Используйте команду **no interface vlan** для удаления интерфейса 3-го уровня.

Интерфейс канала порта автоматически создается, когда для интерфейса физического порта настроена команда **channel-group**. Интерфейс портового канала автоматически удаляется, если для интерфейса физического порта не настроена команда **channel-group**. Для удаления порт-канала используйте команду **no interface port- channel**.

Интерфейс **L2vlan** используется только для добавления описаний к существующим L2 VLAN. Команда **interface l2vlan** не создает нового интерфейса, равно как и команда **no** не удаляет существующий интерфейс.

### Пример

В данном примере показано, как войти в режим Interface Configuration Mode для Ethernet 1/0/5.

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

В данном примере показано, как войти в режим Interface Configuration Mode для VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan 100
Switch(config-if)#
```

В данном примере показано, как войти в режим Interface Configuration Mode для port-channel 3.

```
Switch# configure terminal
Switch(config)# interface port-channel3
Switch(config-if)#
```

## 28-4 interface range

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

**interface range** *INTERFACE-ID* [, | -]

#### Параметры

<i>INTERFACE-ID</i>	Указывает идентификатор интерфейса. Идентификатор интерфейса формируется из типа интерфейса и номера интерфейса. Типы интерфейсов следующие следующие: - Ethernet - порт коммутатора Ethernet со всеми различными носителями. - L2vlan - интерфейс IEEE 802.1Q Layer 2 Virtual LAN.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

#### По умолчанию

Нет

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Команда используется для входа в режим Interface Configuration Mode для указанного диапазона интерфейсов. Команды, введенные в режиме Interface Range Mode, применяются ко всем интерфейсам в диапазоне.

#### Пример

В данном примере показано, как войти в режим конфигурации диапазона интерфейсов для портов 1-5 и порта 8.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/1-5,1/0/8
Switch(config-if-range)#
```

## 28-5 show counters

Данная команда используется для отображения информации об интерфейсе.

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

#### Параметры

<b>interface</b> <i>INTERFACE-ID</i>	(Опционально) Укажите интерфейсы, которые будут
--------------------------------------	---

---

отображаться.

---

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Данная команда используется для отображения статистики счетчиков для интерфейса.

#### Пример

В этом примере показано, как отобразить счетчики на порту 1.

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

```
eth1/0/1 counters
```

```
rxHCTotalPkts           : 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
```

```
rxHCPkt1519toMAXOctets      : 0
txHCPkt64Octets             : 0
txHCPkt65to127Octets       : 0
txHCPkt128to255Octets      : 0
txHCPkt256to511Octets      : 0
txHCPkt512to1023Octets     : 0
txHCPkt1024to1518Octets    : 0
txHCPkt1519toMAXOctets     : 0

rxCRCAAlignErrors          : 0
rxUndersizedPkts           : 0
rxOversizedPkts            : 0
rxFragmentPkts             : 0
rxJabbers                   : 0
rxSymbolErrors              : 0
rxMTUDropPkts              : 0

txCollisions                : 0
ifInErrors                  : 0
ifOutErrors                 : 0
ifInDiscards                : 0
ifOutDiscards               : 0
txCoS0DropPkts             : 0
txCoS1DropPkts             : 0
txCoS2DropPkts             : 0
txCoS3DropPkts             : 0
txCoS4DropPkts             : 0
txCoS5DropPkts             : 0
txCoS6DropPkts             : 0
txCoS7DropPkts             : 0

dot3StatsSingleColFrames   : 0
dot3StatsMultiColFrames    : 0
dot3StatsDeferredTransmissions : 0
dot3StatsLateCollisions    : 0
dot3StatsExcessiveCollisions : 0
dot3StatsFrameTooLongs    : 0

linkChange                  : 0

Switch#
```

## Отображаемые параметры

<b>rxHCTotalPkts</b>	Счетчик принятых пакетов. Возрастает с каждым принятым пакетом (включая поврежденные пакеты, все одноадресные, широковещательные и многоадресные пакеты и пакеты управления MAC).
<b>txHCTotalPkts</b>	Счетчик переданных пакетов. Возрастает с каждым переданным пакетом (включая поврежденные пакеты, все одноадресные, широковещательные и многоадресные пакеты и пакеты управления MAC).
<b>rxHCUnicastPkts</b>	Счетчик принятых пакетов одноадресной рассылки. Возрастает с каждым успешно принятым пакетом одноадресной рассылки.
<b>txHCUnicastPkts</b>	Счетчик переданных пакетов одноадресной рассылки. Возрастает с каждым успешно переданным пакетом одноадресной рассылки.
<b>rxHCMulticastPkts</b>	Счетчик принятых пакетов многоадресной рассылки. Возрастает с каждым успешно принятым пакетом многоадресной рассылки, исключая пакеты управления MAC.
<b>txHCMulticastPkts</b>	Счетчик переданных пакетов многоадресной рассылки. Возрастает с каждым успешно переданным пакетом многоадресной рассылки, исключая пакеты управления MAC.
<b>rxHCBroadcastPkts</b>	Счетчик принятых пакетов широковещательной рассылки. Возрастает с каждым успешно принятым пакетом широковещательной рассылки.
<b>txHCBroadcastPkts</b>	Счетчик переданных пакетов широковещательной рассылки. Возрастает с каждым успешно переданным пакетом широковещательной рассылки.
<b>rxHCOctets</b>	Счетчик принятых байтов. Возрастает с подсчетом байтов принятых пакетов, исключая поврежденные пакеты. (Исключая биты кадров, но включая байты FCS) <b>Примечание:</b> Для усеченного пакета счетчик учитывает только размер max-rcv-frame.
<b>txHCOctets</b>	Счетчик переданных байтов. Возрастает с подсчетом байтов переданных пакетов, исключая поврежденные пакеты. (Исключая биты кадров, но включая байты FCS)
<b>rxHCPkt64Octets</b>	Счетчик принятых 64-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), до 64 байт включительно (исключая биты кадров, но включая байты FCS).
<b>rxHCPkt65to127Octets</b>	Счетчик принятых 64 – 127-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 65 до 127 байт

	включительно (исключая биты кадров, но включая байты FCS).
<b>rxHCPkt128to255Octets</b>	Счетчик принятых 128 – 255-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 128 до 255 байт включительно (исключая биты кадров, но включая байты FCS).
<b>rxHCPkt256to511Octets</b>	Счетчик принятых 256 – 511-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 256 до 511 байт включительно (исключая биты кадров, но включая байты FCS).
<b>rxHCPkt512to1023Octets</b>	Счетчик принятых 512 – 1023-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 512 до 1023 байт включительно (исключая биты кадров, но включая байты FCS).
<b>rxHCPkt1024to1518Octets</b>	Счетчик принятых 1024 – 1518-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 1024 до 1518 байт включительно (исключая биты кадров, но включая байты FCS).
<b>rxHCPkt1519to1522Octets</b>	Счетчик принятых допустимых 1519 – 1522-байтовых кадров VLAN. Возрастает с каждым допустимым принятым кадром VLAN (исключая FCS, Symbol, ошибка Truncated), от 1519 до 1522 байт включительно (исключая биты кадров, но включая байты FCS). Подсчитываются как одиночные, так и дваждытегированные кадры.
<b>rxHCPkt1519to2047Octets</b>	Счетчик принятых 1519 – 2047-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 1519 до 2047 байт включительно (исключая биты кадров, но включая байты FCS).
<b>rxHCPkt2048to4095Octets</b>	Счетчик принятых 2048 – 4095-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 2048 до 4095 байт включительно (исключая биты кадров, но включая байты FCS).
<b>rxHCPkt4096to9216Octets</b>	Счетчик принятых 4096 – 9216-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 4096 до 9216 байт включительно (исключая биты кадров, но включая байты FCS).
<b>rxHCPkt9217to16383Octets</b>	Счетчик принятых 9217 – 16383-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 9217 до 16383 байт включительно (исключая биты кадров, но включая байты FCS).
<b>txHCPkt64Octets</b>	Счетчик переданных 64-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром

	(включая FCS, Symbol, ошибка Len/Type), до 64 байт включительно (исключая биты кадров, но включая байты FCS).
<b>txHCPkt65to127Octets</b>	Счетчик переданных 65 – 127-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 65 до 127 байт включительно (исключая биты кадров, но включая байты FCS).
<b>txHCPkt128to255Octets</b>	Счетчик переданных 128 – 255-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 128 до 255 байт включительно (исключая биты кадров, но включая байты FCS).
<b>txHCPkt256to511Octets</b>	Счетчик переданных 256 – 511-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 256 до 511 байт включительно (исключая биты кадров, но включая байты FCS).
<b>txHCPkt512to1023Octets</b>	Счетчик переданных 512 – 1023-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 512 до 1023 байт включительно (исключая биты кадров, но включая байты FCS).
<b>txHCPkt1024to1518Octets</b>	Счетчик переданных 1024 – 1518-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 1024 до 1518 байт включительно (исключая биты кадров, но включая байты FCS).
<b>txHCPkt1519to1522Octets</b>	Счетчик переданных допустимых 1519 – 1522-байтовых кадров VLAN. Возрастает с каждым допустимым кадром VLAN (исключая FCS, Symbol, ошибку TX), от 1519 до 1522 байт включительно (исключая биты кадров, но включая байты FCS).
<b>txHCPkt1519to2047Octets</b>	Счетчик переданных 1519 – 2047-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 1519 до 2047 байт включительно (исключая биты кадров, но включая байты FCS).
<b>txHCPkt2048to4095Octets</b>	Счетчик переданных 2048 – 4095-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 2048 до 4095 байт включительно (исключая биты кадров, но включая байты FCS).
<b>txHCPkt4096to9216Octets</b>	Счетчик переданных 4096 – 9216-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 4096 до 9216 байт включительно (исключая биты кадров, но включая байты FCS).
<b>txHCPkt9217to16383Octets</b>	Счетчик переданных 9217 – 16383-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 9217 до 16383 байт включительно (исключая



	биты кадров, но включая байты FCS).
<b>rxCRCAAlignErrors</b>	Счетчик принятых кадров с ошибкой выравнивания. Возрастает с каждым принятым пакетом от 64 до max-rcv-frame-size (или max-rcv-frame-size+4 для тегированных кадров) октетов в длину (исключая биты кадра, но включая октеты FCS), но имеющим либо поврежденный FCS с целым числом октетов (ошибка FCS), либо поврежденный FCS с не целым числом октетов (Ошибка выравнивания).
<b>rxUndersizedPkts</b>	Счетчик принятых кадров неполного размера. Возрастает с каждым принятым пакетом меньше 64 байт в длину (исключая биты кадров, но включая октеты FCS), но в остальном сформированным верно (содержащим допустимый FCS).
<b>rxFragmentPkts</b>	Счетчик принятых фрагментов. Возрастает с каждым принятым пакетом меньше 64 байт в длину (исключая биты кадров, но включая октеты FCS), но имеющим либо поврежденный FCS с целым числом октетов (ошибка FCS), либо поврежденный FCS с не целым числом октетов (Ошибка выравнивания).
<b>rxSymbolErrors</b>	Счетчик принятых кадров с ошибкой кода. Возрастает с каждым принятым кадром, содержащим недопустимый символ данных, но допустимый носитель.
<b>txCollisions</b>	Счетчик общего числа коллизий при передаче. Возрастает с общим числом коллизий, возникших во время передачи.
<b>ifInErrors</b>	Счетчик принятых пакетов с ошибкой. Возрастает при приеме пакетов, содержащих ошибки, не допускающие их дальнейшую передачу протоколу на уровень выше. Счетчик является суммой dot3StatsAlignmentErrors, dot3StatsFCSerrors, dot3StatsFrameTooLongs и dot3StatsInternalReceiveError.
<b>ifOutErrors</b>	Счетчик пакетов, переданных с ошибкой. Возрастает при попытке передачи пакетов, содержащих ошибки, не допускающих их дальнейшую передачу. Счетчик является суммой dot3StatsSQETestErrors, dot3StatsLateCollisions, dot3StatsExcessiveCollisions, dot3StatsInternalMacTransmitErrors и dot3StatsCarrierSenseErrors.
<b>ifInDiscards</b>	Счетчик отброшенных принятых пакетов. Возрастает при приеме пакетов, которые в дальнейшем отбрасываются по какой-либо причине. Например, MTU drop, Buffer Full Drop, ACL Drop, Multicast Drop, VLAN Ingress Drop, Invalid IPv6, STP Drop, Storm and FDB Discard и т.д.
<b>ifOutDiscards</b>	Счетчик отброшенных переданных пакетов. Возрастает при передаче пакетов, отброшенных в дальнейшем по какой-либо причине. Например, excessive transit delay discards, HOL drop, STP drop, MTU drop, VLAN drop, и т.д.
<b>txDelayExceededDiscards</b>	Счетчик просроченных переданных пакетов. Возрастает при передаче пакетов, которые были отброшены из-за превышения времени передачи.
<b>txCRC</b>	Счетчик переданных пакетов с ошибкой FCS. Возрастает с каждым переданным пакетом, не прошедшим проверку

	FCS.
<b>dot3StatsSingleColFrames</b>	Счетчик переданных кадров с одиночной коллизией. Доступен только для режима 10/100. Возрастает с каждым переданным кадром, испытавшим одну коллизию во время передачи.
<b>dot3StatsDeferredTransmissions</b>	Счетчик одиночных отложенных при передаче кадров. Доступен только в режиме 10/100. Возрастает с каждым переданным кадром, который был отложен при первой попытке передачи и в дальнейшем не подвергся коллизии во время последующей передачи.
<b>dot3StatsLateCollisions</b>	Счетчик кадров поздней коллизии. Доступен только в режиме 10/100. Возрастает с каждым переданным кадром с поздней коллизией во время попытки передачи.
<b>dot3StatsExcessiveCollisions</b>	Счетчик переданных кадров с избытком коллизий. Доступен только в режиме 10/100. Возрастает с каждым кадром, передача которого не состоялась из-за избытка коллизий.
<b>dot3StatsFrameTooLongs</b>	Счетчик принятых кадров слишком большой длины. Возрастает с каждым принятым кадром, превышающим размер max-rcv-frame-size.

## 28-6 show interfaces

Данная команда используется для просмотра информации об интерфейсе.

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

### Параметры

<i>INTERFACE-ID</i>	(Опционально) Укажите физический порт, VLAN, интерфейс loorbask или другой интерфейс.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Если интерфейс не указан, отображаться будут данные для всех интерфейсов.

### Пример

В данном примере показано, как включить отображение информации об интерфейсе VLAN для интерфейса VLAN 1.

```
Switch# show interfaces vlan1

VLAN1 is enabled, link status is down
Interface type: VLAN
Interface description: VLAN 1 for MIS
MAC address: 08-00-01-22-00-00

Switch#
```

В этом примере показано, как отобразить информацию об интерфейсе для порта 1.

```
Switch#show interfaces eth1/0/1

Eth1/0/1 is enabled, link status is up
  Interface type: 1000BASE-T
  Interface description:
  MAC Address: 00-01-02-03-04-01
  Auto-duplex, auto-speed, auto-mdix
  Send flow-control: off, receive flow-control: off
  Send flow-control oper: off, receive flow-control oper: off
  Full-duplex, 1Gb/s
  Maximum transmit unit: 1536 bytes
  Rx rate: 0 bytes/sec, TX rate: 0 bytes/sec
  RX bytes: 116316, TX bytes: 132495
  RX rate: 0 packets/sec, TX rate: 0 packets/sec
  RX packets: 1213, TX packets: 365
  RX multicast: 774, RX broadcast: 439
  RX CRC error: 0, RX undersize: 0
  RX oversized: 0, RX fragment: 0
  RX jabber: 0, RX dropped Pkts: 1212
  RX MTU exceeded: 0
  TX CRC error: 0, TX excessive deferral: 0
  TX single collision: 0, TX excessive collision: 0
  TX late collision: 0, TX collision:0

Switch#
```

## 28-7 show interfaces counters

Данная команда используется для отображения счетчиков на определенных интерфейсах.

```
show interfaces [INTERFACE-ID [, | -]] counters [errors]
```

**Параметры**

<i>INTERFACE-ID</i>	(Опционально) Укажите, является ли интерфейс физическим портом или интерфейсом VLAN. Если интерфейс не указан, отображаться будут счетчики для всех интерфейсов.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
<b>errors</b>	(Опционально) Укажите для отображения счетчика ошибок.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Данная команда используется для отображения общих счетчиков, счетчиков ошибок или архивной информации для указанного или всех интерфейсов.

**Пример**

В этом примере показано, как отобразить счетчики портов коммутатора на портах с 1 по 8.

```
Switch#show interfaces ethernet 1/0/1-8 counters
```

Port	InOctets / InUcastPkts	InMcastPkts / InBcastPkts
eth1/0/1	1834520 9234	629 338
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 / OutUcastPkts	OutMcastPkts / OutBcastPkts
eth1/0/1	5387265 9381	0 0
eth1/0/2	0 0	0 0
eth1/0/3	0 0	0 0
eth1/0/4	0 0	0 0
eth1/0/5	0 0	0 0
eth1/0/6	0 0	0 0
eth1/0/7	0 0	0 0
eth1/0/8	0 0	0 0

Total Entries:8

Switch#

В этом примере показано, как отобразить счетчики ошибок портов коммутатора.

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

Port	Align-Err	Fcs-Err	Rcv-Err	Undersize	Xmit-Err	OutDiscard
eth1/0/1	0	0	0	0	0	0
eth1/0/2	0	0	0	0	0	0
eth1/0/3	0	0	0	0	0	0
eth1/0/4	0	0	0	0	0	0
eth1/0/5	0	0	0	0	0	0
eth1/0/6	0	0	0	0	0	0
eth1/0/7	0	0	0	0	0	0
eth1/0/8	0	0	0	0	0	0

Port	Single-Col	Multi-Col	Late-Col	Excess-Col	Carri-Sen	Runts
eth1/0/1	0	0	0	0	0	0
eth1/0/2	0	0	0	0	0	0
eth1/0/3	0	0	0	0	0	0
eth1/0/4	0	0	0	0	0	0
eth1/0/5	0	0	0	0	0	0
eth1/0/6	0	0	0	0	0	0
eth1/0/7	0	0	0	0	0	0
eth1/0/8	0	0	0	0	0	0

Port	Giants	Symbol-Err	SQETest-Err	DeferredTx	IntMacTx	IntMacRx
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

```
Total Entries:8
```

```
Switch#
```

### Отображаемые параметры

#### Rcv-Err

Обратитесь к «ifInErrors» в разделе «Отображаемые параметры» команды **show counters**.

#### UnderSize

Обратитесь к «rxUndersizedPkts» в разделе «Отображаемые параметры» команды **show counters**.

<b>Xmit-Err</b>	Обратитесь к «ifOutErrors» в разделе «Отображаемые параметры» команды <b>show counters</b> .
<b>OutDiscard</b>	Обратитесь к «ifOutDiscards» в разделе «Отображаемые параметры» команды <b>show counters</b> .
<b>Single-Col</b>	Обратитесь к «dot3StatsSingleColFrames» в разделе «Отображаемые параметры» команды <b>show counters</b> .
<b>Multi-Col</b>	Обратитесь к «dot3StatsMultiColFrames» в разделе «Отображаемые параметры» команды <b>show counters</b> .
<b>Late-Col</b>	Обратитесь к «dot3StatsLateCollisions» в разделе «Отображаемые параметры» команды <b>show counters</b> .
<b>Excess-Col</b>	Обратитесь к «dot3StatsExcessiveCollisions» в разделе «Отображаемые параметры» команды <b>show counters</b> .
<b>Symbol-Err</b>	Обратитесь к «rxSymbolErrors» в разделе «Отображаемые параметры» команды <b>show counters</b> .
<b>DeferredTx</b>	Обратитесь к «txDelayExceededDiscards» в разделе «Отображаемые параметры» команды <b>show counters</b> .
<b>IntMacTx</b>	Обратитесь к «dot3StatsInternalMacTransmitErrors» в разделе «Отображаемые параметры» команды <b>show counters</b> .
<b>IntMacRx</b>	Обратитесь к пункту "dot3StatsInternalMacReceiveErrors" в команде <b>show counters</b> .
<b>Align-Err</b>	Обратитесь к пункту "dot3StatsAlignmentErrors" в команде <b>show counters</b> .
<b>Fcs-Err</b>	Обратитесь к пункту "dot3StatsFCSErrors" в команде <b>show counters</b> .

## 28-8 show interfaces status

Данная команда используется для просмотра состояния подключения портов коммутатора.

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

### Параметры

<i>INTERFACE-ID</i>	(Опционально) Укажите interface ID. Если параметр не указан, отображаться будет состояние подключения всех портов коммутатора.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

## Использование команды

Используйте эту команду для отображения состояния подключения портов коммутатора. Если параметр не указан, будет отображено состояние подключения всех портов коммутатора.

## Пример

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

```
Switch# show interfaces eth1/0/1-8 status
```

Port	Status	VLAN	Duplex	Speed	Type
eth1/0/1	not-connected	1	auto	auto	1000BASE-T
eth1/0/2	not-connected	1	auto	auto	1000BASE-T
eth1/0/3	not-connected	1	auto	auto	1000BASE-T
eth1/0/4	not-connected	1	auto	auto	1000BASE-T
eth1/0/5	not-connected	1	auto	auto	1000BASE-T
eth1/0/6	not-connected	1	auto	auto	1000BASE-T
eth1/0/7	not-connected	1	auto	auto	1000BASE-T
eth1/0/8	connected	trunk	a-full	a-1000	1000BASE-T

```
Total Entries: 8
Switch#
```

## 28-9 show interfaces utilization

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

### Параметры

<i>INTERFACE-ID</i>	(Опционально) Укажите interface ID. Если параметр не указан, отображаться будет информация о загрузке всех физических портов коммутатора.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
<b>utilization</b>	Указывает на отображение информации об использовании.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode



**Использование команды**

Используйте эту команду для отображения загрузки портов коммутатора.

**Пример**

В этом примере показано, как отобразить загрузку 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#
```

**28-10 show interfaces auto-negotiation**

Данная команда используется для просмотра подробной информации об автосогласовании на физическом порту.

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

**Параметры**

<i>INTERFACE-ID</i>	(Опционально) Укажите interface ID. Если параметр не указан, отображаться будет информация обо всех физических портах.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
<b>auto-negotiation</b>	Укажите для отображения подробной информации об автосогласовании.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Данная команда используется для просмотра детальной информации об автосогласовании.

**Пример**

В данном примере показано отображение информации об автосогласовании.

```
Switch# show interfaces eth1/0/1-2 auto-negotiation

eth1/0/1
Auto Negotiation: Disabled

eth1/0/2
Auto Negotiation: Enabled

Speed auto downgrade: Disabled
Remote Signaling: Detected
Configure Status: Configuring
Capability Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
Capability Advertised Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
Capability Received Bits: -
RemoteFaultAdvertised: Disabled
RemoteFaultReceived: NoError

Switch#
```

**28-11 show interfaces description**

Данная команда используется для просмотра описания и состояния интерфейсов.

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

**Параметры**

<i>INTERFACE-ID</i>	(Опционально) Укажите interface ID. Если параметр не указан, отображаться будет информация о всех интерфейсах.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

<b>description</b>	Укажите для отображения описания и состояния интерфейсов.
--------------------	---

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Данная команда используется для просмотра описания и состояния интерфейсов.

**Пример**

В данном примере показано отображение описания и состояния интерфейсов.

```
Switch#show interfaces description

Interface          Status      Administrative  Description
-----
eth1/0/1           up          enabled
eth1/0/2           down        enabled
eth1/0/3           down        enabled
eth1/0/4           down        enabled
eth1/0/5           down        enabled
eth1/0/6           down        enabled
eth1/0/7           down        enabled
eth1/0/8           down        enabled
eth1/0/9           down        enabled
eth1/0/10          down        enabled        Physical Port 10
eth1/0/11          down        enabled
eth1/0/12          down        enabled
eth1/0/13          down        enabled
eth1/0/14          down        enabled
eth1/0/15          down        enabled
eth1/0/16          down        enabled
eth1/0/17          down        enabled
eth1/0/18          down        enabled
eth1/0/19          down        enabled
eth1/0/20          down        enabled
eth1/0/21          down        enabled

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

**28-12 shutdown**

Данная команда используется для отключения интерфейса. При использовании формы **no** включит включит интерфейс.

**shutdown**

## no shutdown

### Параметры

Нет

### По умолчанию

По умолчанию выбрана опция **no shutdown**.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Эта команда доступна для конфигурации физического порта и интерфейса VLAN. Эта команда также настраивается для портов-членов портового канала.

Команда заставит порт перейти в отключенное состояние. В отключенном состоянии порт не сможет принимать или передавать пакеты. Использование команды **no shutdown** вернет порт во включенное состояние. При отключении порта статус соединения также будет отключен.

### Пример

В данном примере показано, как отключить порт 1/0/1 с помощью данной команды.

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

## 29. . Команды Internet Group Management Protocol (IGMP) Snooping

### 29-1 clear ip igmp snooping statistics

Данная команда используется для удаления статистики IGMP Snooping.

```
clear ip igmp snooping statistics {all | vlan VLAN-ID | interface INTERFACE-ID}
```

#### Параметры

<b>all</b>	Укажите, чтобы удалить статистику IP IGMP Snooping для всех VLAN и портов.
<b>vlan VLAN-ID</b>	Укажите VLAN, для которой необходимо удалить статистику IP IGMP Snooping.
<b>interface INTERFACE-ID</b>	Укажите порт, для которого необходимо удалить статистику IP IGMP Snooping.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте данную команду, чтобы удалить статистику IGMP Snooping.

#### Пример

В данном примере показано, как удалить всю статистику IGMP Snooping.

```
Switch# clear ip igmp snooping statistics all
Switch#
```

### 29-2 ip igmp snooping

Данная команда используется для включения функции IGMP Snooping на коммутаторе. Используйте форму **no**, чтобы отключить данную функцию.

```
ip igmp snooping
no ip igmp snooping
```

#### Параметры

Нет

**По умолчанию**

IGMP snooping отключен на всех интерфейсах VLAN.  
Глобальное состояние IGMP snooping по умолчанию отключено.

**Режим ввода команды**

VLAN Configuration Mode  
Global Configuration Mode

**Использование команды**

В режиме Interface Configuration Mode команда может быть использована только для настройки интерфейса VLAN. Для того, чтобы предоставить VLAN доступ к IGMP Snooping, необходимо включить данную функцию глобально и для интерфейса. Настройки IGMP Snooping и MLD Snooping являются независимыми и могут быть применены для VLAN одновременно.

**Пример**

В этом примере показано, как глобально отключить IGMP snooping.

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

В этом примере показано, как включить IGMP snooping глобально.

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

В этом примере показано, как отключить IGMP snooping в сети VLAN 1.

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

**29-3 ip igmp snooping fast-leave**

Данная команда используется для настройки функции IGMP Snooping Fast Leave на интерфейсе. Используйте форму **no**, чтобы отключить данную функцию на указанном интерфейсе.

**ip igmp snooping fast-leave**  
**no ip igmp snooping fast-leave**

**Параметры**

Нет

**По умолчанию**

По умолчанию данная опция отключена.

**Режим ввода команды**

VLAN Configuration Mode

**Использование команды**

Данная команда может применяться только для настройки интерфейса VLAN. Используйте команду **ip igmp snooping fast-leave**, чтобы удалить членство IGMP на порту после получения сообщения Leave, не применяя механизм обработки сообщений Group-Specific Query (с указанием группы) или Group-Source-Specific Query (с указанием источника группы).

**Пример**

В данном примере показано, как включить функцию IGMP Snooping Fast Leave на VLAN 1.

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

**29-4 ip igmp snooping last-member-query-interval**

Данная команда используется для настройки интервала, через который IGMP snooping querier посылает IGMP сообщения с запросами, специфичными для группы или источника группы (канала). Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

**ip igmp snooping last-member-query-interval SECONDS**  
**no ip igmp snooping last-member-query-interval**

**Параметры**

<i>SECONDS</i>	Укажите максимальный интервал между сообщениями Group-Specific Query, включая отправленные в ответ на сообщения Leave Group. Доступный диапазон значений: от 1 до 25.
----------------	---

**По умолчанию**

Значение по умолчанию – 1 секунда.

**Режим ввода команды**

VLAN Configuration Mode

**Использование команды**

Данная команда может применяться только для настройки интерфейса VLAN. Получив сообщение IGMP Leave, IGMP Snooping Querier будет считать, что на интерфейсе нет локальных участников, если по истечении времени ожидания не будет получено ни одного ответа. Пользователи могут уменьшить данный интервал, чтобы сократить время, которое уходит у коммутатора на обнаружение потери последнего участника группы.

**Пример**

В данном примере показано, как настроить значение last member query interval. Указанное значение – 3 секунды.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping last-member-query-interval 3
Switch(config-vlan)#
```

## 29-5 ip igmp snooping mrouter

Эта команда используется для настройки указанного интерфейса(ов) в качестве портов маршрутизатора многоадресной рассылки или запрещенных портов маршрутизатора многоадресной рассылки на коммутаторе. Используйте форму **no** этой команды, чтобы удалить интерфейс(ы) из портов маршрутизатора или запрещенных портов маршрутизатора многоадресной рассылки.

**ip igmp snooping mrouter {interface *INTERFACE-ID* [, | -] | forbidden interface *INTERFACE-ID* [, | -]}**  
**no ip igmp snooping mrouter {interface *INTERFACE-ID* [, | -] | forbidden interface *INTERFACE-ID* [, | -]}**

### Параметры

<b>interface</b>	Укажите статический multicast router-порт.
<b>forbidden interface</b>	Укажите порт, который не может быть multicast router-портом.
<i>INTERFACE-ID</i>	Укажите интерфейс или список интерфейсов. В качестве интерфейса может быть использован физический порт или port-channel.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

### По умолчанию

Порт многоадресного маршрутизатора IGMP snooping не настроен.

### Режим ввода команды

VLAN Configuration Mode

### Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. multicast router-портом можно назначить физический порт или port-channel. Указанный multicast router-порт должен являться портом-участником сконфигурированной VLAN. Multicast router-порт может быть изучен динамически или сконфигурирован статически. При помощи динамического изучения устройство IGMP Snooping будет изучать пакеты IGMP, PIM или DVMRP, чтобы идентифицировать multicast router-порт. Если автоматическое изучение отключено, multicast router-порт может быть только сконфигурирован статически.

### Пример



В этом примере показано, как создать порт статического маршрутизатора многоадресной рассылки IGMP snooping для VLAN 1.

```
Switch#configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping mrouter interface eth1/0/4
Switch(config-vlan)#
```

## 29-6 ip igmp snooping querier

Данная команда используется для указания устройства в качестве IGMP Snooping Querier. Используйте форму **no**, чтобы отключить данную функцию.

```
ip igmp snooping querier
no ip igmp snooping querier
```

### Параметры

Нет

### По умолчанию

По умолчанию данная функция отключена.

### Режим ввода команды

VLAN Configuration Mode

### Использование команды

Если система может играть роль querier, она будет прослушивать пакеты IGMP-запросов, отправленные другими устройствами. Если сообщение запроса IGMP получено, устройство с меньшим значением IP-адреса становится querier.

### Пример

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

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

## 29-7 ip igmp snooping query-interval

Эта команда используется для настройки интервала, через который IGMP snooping querier периодически отправляет сообщения общего запроса IGMP. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

```
ip igmp snooping query-interval SECONDS
no ip igmp snooping query-interval
```

**Параметры**

<i>SECONDS</i>	Укажите интервал между сообщениями IGMP General Query для обозначенного маршрутизатора. Доступный диапазон значений: от 1 до 31744.
----------------	---

**По умолчанию**

Значение по умолчанию – 125 секунд.

**Режим ввода команды**

VLAN Configuration Mode

**Использование команды**

Данная команда может применяться только для настройки интерфейса VLAN. Query Interval – это интервал между сообщениями General Query, отправленными Querier. Администратор может настраивать количество IGMP-сообщений, изменяя значение данного интервала: чем больше значение интервала, тем реже будут отправляться сообщения IGMP Query.

**Пример**

В данном примере показано, как настроить интервал IGMP Snooping Query на VLAN 1000. Указанное значение – 300 секунд.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping query-interval 300
Switch(config-vlan)#
```

**28-8 ip igmp snooping query-max-response-time**

Данная команда используется для настройки максимального значения времени ожидания, анонсированного в сообщениях IGMP Snooping Query. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip igmp snooping query-max-response-time SECONDS
no ip igmp snooping query-max-response-time
```

**Параметры**

<i>SECONDS</i>	Укажите максимальное значение времени ожидания, анонсированное в сообщениях IGMP Snooping Query. Доступный диапазон значений: от 1 до 25 секунд.
----------------	--

**По умолчанию**

Значение по умолчанию – 10 секунд.

**Режим ввода команды**

## VLAN Configuration Mode

**Использование команды**

Используйте эту команду для настройки периода, в течение которого член группы может отвечать на сообщение запроса IGMP, прежде чем IGMP Snooping удалит его принадлежность к группе.

**Пример**

В данном примере показано, как настроить максимальное значение времени ожидания на интерфейсе. Указанное значение – 20 секунд.

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

**29-9 ip igmp snooping query-version**

Данная команда используется для настройки версии пакетов General Query, отправляемых IGMP Snooping Querier. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip igmp snooping query-version NUMBER
no ip igmp snooping query-version
```

**Параметры**

<i>NUMBER</i>	Укажите версию пакета IGMP General Query, отправленного IGMP Snooping Querier. Доступный диапазон значений: от 1 до 3.
---------------	--

**По умолчанию**

Значение по умолчанию – 3.

**Режим ввода команды**

## VLAN Configuration Mode

**Использование команды**

Данная команда может применяться только для настройки интерфейса VLAN. Настройки версии пакета Query повлияют на выбор Querier. Если выбрана версия 1, IGMP Snooping действует в качестве Querier и не инициирует выбор нового Querier вне зависимости от того, какой пакет IGMP Query получен. Если выбрана версия 2 или 3, IGMP Snooping инициирует выбор нового Querier при получении пакета IGMPv2 или IGMPv3, и не инициирует выбор нового Querier при получении пакета IGMPv1.

**Пример**

В данном примере показано, как настроить версию пакета Query на VLAN 1000. Указанная версия – 2.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping query-version 2
Switch(config-vlan)#
```

## 29-10 ip igmp snooping robustness-variable

Данная команда используется для настройки robustness variable (переменной надежности), используемой в IGMP Snooping. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip igmp snooping robustness-variable VALUE
no ip igmp snooping robustness-variable
```

### Параметры

VALUE	Укажите значение robustness variable в диапазоне от 1 до 7.
-------	---

### По умолчанию

Значение по умолчанию – 2.

### Режим ввода команды

VLAN Configuration Mode

### Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Robustness variable обеспечивает точную настройку в соответствии с ожидаемой потерей пакетов на интерфейсе. Значение robustness variable используется для расчета следующих интервалов IGMP-сообщений:

- **Group member interval** – промежуток времени, по истечении которого маршрутизатор считает, что в группе больше нет активных участников. Данный интервал рассчитывается следующим образом:  $(\text{robustness variable} \times \text{query interval}) + (1 \times \text{query response interval})$ .
- **Other querier present interval** – промежуток времени, по истечении которого многоадресный маршрутизатор считает, что маршрутизатор, являющийся Querier, больше не доступен. Данный интервал рассчитывается следующим образом:  $(\text{robustness variable} \times \text{query interval}) + (0.5 \times \text{query response interval})$ .
- **Last member query count** – количество запросов Group-Specific Queries (с указанием группы), отправленных маршрутизатором до того, как он предполагает, что в группе нет локальных участников. Robustness variable является значением по умолчанию данного счетчика.

Пользователи могут увеличить данное значение, если для сети требуются более свободные условия.

### Пример

В данном примере показано, как настроить robustness variable на интерфейсе VLAN 1000. Указанное значение – 3.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping robustness-variable 3
Switch(config-vlan)#
```

## 29-11 ip igmp snooping static-group

Данная команда используется для настройки статической группы IGMP Snooping. Используйте форму **no**, чтобы удалить статическую группу.

**ip igmp snooping static-group** *GROUP-ADDRESS* **interface** *INTERFACE-ID* [, | -]  
**no ip igmp snooping static-group** *GROUP-ADDRESS* [**interface** *INTERFACE-ID* [, | -]]

### Параметры

<i>GROUP-ADDRESS</i>	Укажите IP-адрес многоадресной группы.
<b>interface</b> <i>INTERFACE-ID</i>	Укажите интерфейс или список интерфейсов. Доступны физические порты или port-channel.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

### По умолчанию

По умолчанию статическая группа не настроена.

### Режим ввода команды

VLAN Configuration Mode

### Использование команды

Используйте эту команду для создания статической группы IGMP snooping в случае, если подключенный хост не поддерживает протокол IGMP.

### Пример

В данном примере показано, как добавить запись статической группы и источник multicast потока для IGMP Snooping.

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

## 29-12 ip igmp snooping minimum-version

Данная команда используется для настройки минимальной версии IGMP-узлов, разрешенной на интерфейсе. Используйте форму **no**, чтобы удалить ограничение.

**ip igmp snooping minimum-version {2 | 3}**  
**no ip igmp snooping minimum-version**

#### Параметры

<b>2</b>	Укажите, чтобы отфильтровать сообщения IGMPv1.
<b>3</b>	Укажите, чтобы отфильтровать сообщения IGMPv1 и IGMPv2.

#### По умолчанию

По умолчанию ограничения минимальной версии отсутствуют.

#### Режим ввода команды

VLAN Configuration Mode

#### Использование команды

Эта настройка применяется только для фильтрации отчетов о членстве в IGMP.

#### Пример

В данном примере показано, как ограничить подключение всех узлов IGMPv1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping minimum-version 2
Switch(config-vlan)#
```

В данном примере показано, как ограничить подключение всех узлов IGMPv1 и IGMPv2.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping minimum version 3
Switch(config-vlan)#
```

В данном примере показано, как удалить ограничения, сконфигурированные на VLAN 1.

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

## 29-13 show ip igmp snooping

Данная команда используется для отображения информации об IGMP Snooping на коммутаторе.

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

**Параметры**


---

<b>vlan</b> <i>VLAN-ID</i>	(Опционально) Укажите VLAN, которую необходимо отобразить.
----------------------------	--

---

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте эту команду для отображения информации IGMP snooping для всех VLAN, где IGMP snooping включен.

**Пример**

В данном примере показано, как отобразить настройки IGMP Snooping.

```
Switch#show ip igmp snooping

IGMP snooping global state: Enabled

Switch#
```

В этом примере показано, как отобразить информацию IGMP snooping для VLAN 2.

```
Switch#show ip igmp snooping vlan 2

VLAN #2 configuration
  IGMP snooping state           : Disabled
  Minimum version               : v1
  Fast leave                    : Disabled (port-based)
  Querier state                 : Disabled
  Query version                 : v3
  Query interval                : 125 seconds
  Max response time             : 10 seconds
  Robustness value              : 2
  Last member query interval    : 1 seconds

Total Entries: 1

Switch#
```

## 29-14 show ip igmp snooping groups

Данная команда используется для отображения информации о группе IGMP Snooping, изученной на коммутаторе.

**show ip igmp snooping groups [vlan VLAN-ID | IP-ADDRESS]**

### Параметры

<b>vlan VLAN-ID</b>	(Опционально) Укажите интерфейс VLAN, который будет отображаться. Если VLAN не указан, будет отображаться информация о группах IGMP snooping всех VLAN.
<b>IP-ADDRESS</b>	(Опционально) Указывает IP-адрес группы, который будет отображаться. Если IP-адрес не указан, будет отображаться вся информация о группе IGMP.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте эту команду для отображения информации о группе IGMP snooping.

### Пример

В этом примере показано, как отобразить информацию о группе IGMP snooping.

```
Switch# show ip igmp snooping groups

IGMP Snooping Connected Group Membership:

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

Total Entries: 1

Switch#
```

### Отображаемые параметры

<b>FM</b>	Filter Mode (Режим фильтрации): Значение режима фильтрации может быть либо IN (Включить), либо EX (Исключить). EX - Режим фильтрации - Исключить.
-----------	--



---

 IN - Режим фильтрации - Включить.
 

---

**Exp (sec)****Expire time** (Время истечения): Время в секундах до истечения срока действия записи.

## 29-15 show ip igmp snooping mrouter

Эта команда используется для отображения информации о портах маршрутизатора IGMP snooping, изученных и настроенных на коммутаторе.

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

### Параметры

---

**vlan VLAN-ID**

 (Опционально) Указывает VLAN для отображения. Если VLAN не указана, будет отображаться информация IGMP snooping для всех VLAN.
 

---

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Уровень команды по умолчанию

Уровень 1

### Использование команды

Используйте эту команду для отображения динамически обучаемых или вручную настроенных интерфейсов маршрутизаторов многоадресной рассылки.

Если параметр не указан, будет отображена информация IGMP snooping по всем VLAN.

### Пример

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

```
Switch# show ip igmp snooping mrouter
```

```

VLAN      Ports
-----
1         3/0/3-3/0/4 (static)
          3/0/6 (forbidden)
          4/0/2 (dynamic)
2         4/0/4 (static)
          4/0/3 (dynamic)

```

```
Total Entries: 2
```

```
Switch#
```

## 29-16 show ip igmp snooping static-group

Данная команда используется для отображения статически настроенных групп IGMP Snooping на коммутаторе.

```
show ip igmp snooping static-group [GROUP-ADDRESS | vlan VLAN-ID]
```

### Параметры

<i>GROUP-ADDRESS</i>	(Опционально) Укажите IP-адрес группы, которую необходимо отобразить.
<b>vlan</b> <i>VLAN-ID</i>	(Опционально) Укажите VLAN ID, который необходимо отобразить.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте данную команду, чтобы отобразить статически настроенные группы IGMP Snooping на коммутаторе. Если дополнительные параметры не выбраны, будет отображена вся информация.

### Пример

В данном примере показано, как отобразить статически настроенные группы IGMP Snooping.

```
Switch#show ip igmp snooping static-group
```

```
VLAN ID  Group address  Interface
-----  -
```

VLAN ID	Group address	Interface
2	226.1.2.2	1/0/3

```
Total Entries: 1
```

```
Switch#
```

## 29-17 show ip igmp snooping statistics

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

```
show ip igmp snooping statistics {interface [INTERFACE-ID [, | -]] | vlan [VLAN-ID [, | -]]}
```

### Параметры

<b>interface</b>	Указывает для отображения счетчиков статистики по интерфейсу.
<i>INTERFACE-ID</i>	(Опционально) Укажите интерфейсы, которые будут отображаться.
<b>vlan</b>	Указывает для отображения счетчиков статистики по VLAN.
<i>VLAN-ID</i>	(Опционально) Указывает идентификатор VLAN, который будет отображаться.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

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

### Пример

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

```
Switch#show ip igmp snooping statistics vlan 1
```

```
VLAN 1 Statistics:
```

```
IGMPv1 Rx: Report 0, Query 0  
IGMPv2 Rx: Report 0, Query 0, Leave 0  
IGMPv3 Rx: Report 3, Query 0  
IGMPv1 Tx: Report 0, Query 0  
IGMPv2 Tx: Report 0, Query 0, Leave 0  
IGMPv3 Tx: Report 1, Query 2
```

```
Total Entries: 1
```

```
Switch#
```

## 30. Команды IP-MAC-Port Binding (IMPВ)

### 30-1 clear ip ip-mac-port-binding violation

Данная команда используется для удаления заблокированных записей IP-MAC-Port Binding (IMPВ).

```
clear ip ip-mac-port-binding violation {all | interface INTERFACE-ID | MAC-ADDRESS}
```

#### Параметры

<b>all</b>	Укажите для удаления всех неразрешенных записей.
<b>interface</b> <i>INTERFACE-ID</i>	Укажите для удаления неразрешенных записей, созданных определенным интерфейсом.
<i>MAC-ADDRESS</i>	Укажите для удаления неразрешенных записей с определенным MAC-адресом.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Команда используется для удаления неразрешенных записей IMPВ 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#
```

### 30-2 ip ip-mac-port-binding

Данная команда используется для включения управления доступом IMPВ для интерфейсов порта. При использовании формы **no** команда отключит функцию управления доступом IMPВ.

```
ip ip-mac-port-binding [MODE]
```

```
no ip ip-mac-port-binding
```

#### Параметры

<i>MODE</i>	Укажите режим управления доступом IMPВ. <b>strict-mode:</b> укажите для включения строгого режима управления доступом (strict). <b>loose-mode:</b> укажите для включения режима управления доступом loose. Если режим не задан, используется <b>strict-</b>
-------------	---

---

**mode.**

---

**По умолчанию**

По умолчанию опция отключена.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Если на порту назначен режим управления доступом IMPV **strict-mode**, узел может получить доступ к порту только после того, как узел отправит ARP или IP-пакеты, и эти пакеты пройдут проверку привязки. Чтобы пройти проверку привязки, IP и MAC-адрес источника, VLAN ID и номер порта назначения должны совпадать с любой записью, определенной либо статической записью привязки IP Source Guard, либо изученной динамической записью привязки DHCP Snooping.

Если на порту назначен режим управления доступом IMPV **loose-mode**, узлу будет отказано в доступе к порту после отправки узлом ARP или IP-пакетов, а эти пакеты, отправленные узлом, не пройдут проверку привязки. Чтобы пройти проверку привязки, IP и MAC-адрес источника, VLAN ID и номер порта назначения должны совпадать с любой записью, определенной либо статической записью привязки IP Source Guard, либо изученной динамической записью привязки DHCP Snooping.

**Пример**

В этом примере показано, как включить контроль доступа в жестком режиме IMPV на порту 10.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/10
Switch(config-if)# ip ip-mac-port-binding strict
Switch(config-if)#
```

**30-3 show ip ip-mac-port-binding**

Данная команда используется для отображения настроек IMPV или записей, заблокированных с помощью управления доступом IMPV.

**show ip ip-mac-port-binding [interface INTERFACE-ID [, | -]] [violation]**

**Параметры**

<b>interface</b> INTERFACE-ID	(Опционально) Укажите для отображения определенного интерфейса.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
<b>violation</b>	(Опционально) Укажите для отображения заблокированной записи.

**По умолчанию**

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте данную команду для отображения настроек IMPV или используйте команду **show ip ip-mac-port-binding violation** для отображения записей, заблокированных из-за нарушения проверки IMPV.

### Пример

В данном примере показано, как включить отображение всех заблокированных записей управления доступом IMPV.

```
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 IMPV 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#
```

## 30-4 snmp-server enable traps ip-mac-port-binding

Данная команда используется для включения уведомлений SNMP для привязки IP-MAC-Port Binding. При использовании формы **no** команда отключит уведомления SNMP.

```
snmp-server enable traps ip-mac-port-binding
no snmp-server enable traps ip-mac-port-binding
```

## Параметры

Нет

## По умолчанию

По умолчанию данная функция отключена.

## Режим ввода команды

Global Configuration Mode

## Использование команды

Используйте эту команду, чтобы включить или отключить отправку SNMP-уведомлений для таких событий. Если команда включена, коммутатор отправляет ловушки нарушений, если получен любой пакет нарушения.

## Пример

В этом примере показано, как включить отправку трапов для IMPV.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps ip-mac-port-binding
Switch(config)#
```

---



## 31. Команды многоадресной рассылки IP (IPMC)

### 31-1 show ip mroute forwarding-cache

Эта команда используется для отображения содержимого базы данных кэша перенаправления многоадресной маршрутизации IP.

```
show ip mroute forwarding-cache [group-addr GROUP-ADDRESS [source-addr SOURCE-ADDRESS]]
```

#### Параметры

<b>group-addr</b> GROUP-ADDRESS	(Опционально) Укажите IP-адрес группы.
<b>source-addr</b> SOURCE-ADDRESS	(Опционально) Указывает IP-адрес источника многоадресной рассылки.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Кэш пересылки IP multicast представляет собой сводку таблицы маршрутов IP multicast, таблицы членов групп IGMP snooping и портов маршрутизаторов multicast.

#### Пример

В этом примере показано, как отобразить кэш переадресации многоадресной маршрутизации IP.

```
Switch# show ip mroute forwarding-cache
(10.1.1.1, 239.0.0.0) VLAN0060
  Outgoing interface list: 1/0/1, T2

(+,225.0.0.0) VLAN0070
  Outgoing interface list: 1/0/1-1/0/2

(10.1.1.1, 239.0.0.1) VLAN0060
  Outgoing interface list: 1/0/1, 2/0/2

Total entries: 3

Switch#
```

**Отображаемые параметры**

<b>239.0.0.0</b>	Адрес группы.
<b>10.1.1.1</b>	Адрес источника.
<b>*</b>	Подстановочный адрес источника.
<b>VLAN0060</b>	Интерфейс, на который поступили многоадресные данные.
<b>Outgoing interface list</b>	Список исходящих интерфейсов для многоадресных данных. Он содержит интерфейсы коммутации 2-го уровня и маршрутизации 3-го уровня.

## 32. Команды IP Multicast версии 6 (IPMv6)

### 32-1 show ipv6 mroute forwarding-cache

Эта команда используется для отображения содержимого базы данных кэша пересылки многоадресной маршрутизации IPv6.

```
show ipv6 mroute forwarding-cache [group-addr GROUP-ADDRESS [source-addr SOURCE-ADDRESS]]
```

#### Параметры

<b>group-addr</b> GROUP-ADDRESS	(Опционально) Указывает IPv6-адрес группы.
<b>source-addr</b> SOURCE-ADDRESS	(Опционально) Указывает IPv6-адрес источника многоадресной рассылки.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Кэш пересылки многоадресной рассылки IPv6 представляет собой сводку таблицы маршрутов многоадресной рассылки IPv6, таблицы членов групп MLD snooping и портов маршрутизаторов многоадресной рассылки.

#### Пример

В этом примере показано, как отобразить кэш пересылки многоадресной маршрутизации IPv6.

```
Switch# show ipv6 mroute forwarding-cache

(2000:60:1:1::10, FF0E::1:1:1) VLAN0060
  Outgoing interface list: 1/0/1, port-channel2

(2000:60:1:1::10, FF0E::1:1:2) VLAN0060
  Outgoing interface list: 1/0/1, 2/0/2

Total entries: 2

Switch#
```

#### Отображаемые параметры

<b>FF0E::1:1:1</b>	Адрес группы.
<b>2000:60:1:1::10</b>	Адрес источника.
<b>VLAN0060</b>	Интерфейс, на который поступили многоадресные данные.
<b>Outgoing interface list</b>	Список исходящих интерфейсов для многоадресных данных. Он содержит интерфейсы коммутации 2-го уровня и маршрутизации 3-го уровня.

## 33. Команды IP Source Guard

### 33-1 ip verify source vlan dhcp-snooping

Данная команда используется для включения IP Source Guard на порту. При использовании формы **no** команда отключит IP Source Guard.

```
ip verify source vlan dhcp-snooping [ip-mac]
no ip verify source vlan dhcp-snooping [ip-mac]
```

#### Параметры

<b>ip-mac</b>	(Опционально) Укажите для проверки и IP, и MAC-адреса получаемых IP-пакетов.
---------------	--

#### По умолчанию

По умолчанию опция отключена.

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

Команда используется для настройки физического порта и port-channel. Используйте команду для включения IP Source Guard на необходимом порту.

При включении на порту IP Source Guard IP-пакеты, приходящие на порт, будут проверяться списком управления доступом (ACL). Порт списка управления доступом (порт ACL) – аппаратный механизм. Его записи могут быть настроены вручную либо получены с помощью таблицы привязки DHCP. Пакет, не прошедший проверку, будет отброшен.

Существует два типа проверки:

- Если не указан ip-mac, проверка основана только на IP-адресе источника и VLAN.
- Если указан ip-mac, проверка основана на MAC-адресе источника, VLAN и IP-адресе источника.

#### Пример

В данном примере показано, как включить IP Source Guard для Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config-if)#
```

### 33-2 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

<i>MAC-ADDRESS</i>	Укажите MAC-адрес для привязки IP-to-MAC.
<b>vlan</b> <i>VLAN-ID</i>	Укажите VLAN, которой принадлежит проверенный узел.
<i>IP-ADDRESS</i>	Укажите IP-адрес для привязки IP-to-MAC.
<b>interface</b> <i>INTERFACE-ID</i>	Укажите порт, к которому подключен проверенный узел.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

#### По умолчанию

Нет

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте эту команду для добавления или удаления записи статической привязки, используемой для проверки защиты источника IP. Параметры, указанные для команды, должны точно соответствовать удаляемой записи.

Если MAC-адрес и VLAN для настроенной записи уже существуют, существующая запись привязки обновляется.

#### Пример

В данном примере показано, как настроить привязку IP Source Guard с IP-адресом 10.1.1.1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 Ethernet 1/0/10.

```
Switch# configure terminal
Switch(config)# ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface ethernet 1/0/10
Switch(config)#
```

В данном примере показано, как удалить привязку IP Source Guard с IP-адресом 10.1.1.1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 Ethernet 1/0/10.

```
Switch# configure terminal
Switch(config)# no ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface ethernet 1/0/10
Switch(config)#
```

### 33-3 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

<i>IP-ADDRESS</i>	(Опционально) Укажите для отображения привязки IP Source Guard на основе IP-адреса.
<i>MAC-ADDRESS</i>	(Опционально) Укажите для отображения привязки IP Source Guard на основе MAC-адреса.
<b>dhcp-snooping</b>	(Опционально) Укажите для отображения привязки IP Source, изученной при помощи DHCP Snooping.
<b>static</b>	(Опционально) Укажите для отображения привязки IP Source Guard, настроенной вручную.
<b>vlan</b> <i>VLAN-ID</i>	(Опционально) Укажите для отображения привязки IP Source Guard на основе VLAN.
<b>interface</b> <i>INTERFACE-ID</i>	(Опционально) Укажите для отображения привязки IP Source Guard на основе порта.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Записи привязки IP Source Guard либо настраиваются вручную, либо изучаются автоматически с помощью DHCP Snooping для защиты IP-трафика.

#### Пример

В данном примере показано, как 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  10.1.1.10      infinite   static         100   eth1/0/3

Total Entries: 1

Switch#
```

В данном примере показано, как настроить отображение привязки IP Source Guard для IP-адреса 10.1.1.11, MAC-адреса 00-01-01-01-01-10 в VLAN 100 на Ethernet 1/0/3 и изучение DHCP Snooping.

```
Switch# show ip source binding 10.1.1.11 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  10.1.1.11      3564       dhcp-snooping 100   eth1/0/3

Total Entries: 1

Switch#
```

### Отображаемые параметры

<b>MAC Address</b>	MAC-адрес клиента.
<b>IP Address</b>	IP-адрес клиента, назначенный DHCP-сервером или настроенный пользователем.
<b>Lease (sec)</b>	Время аренды IP-адреса.
<b>Type</b>	Тип привязки. Статическая привязка настраивается вручную. Динамическая привязка изучается с помощью DHCP Snooping.
<b>VLAN</b>	Номер VLAN, где находится интерфейс клиента.
<b>Interface</b>	Интерфейс, подключаемый к узлу DHCP-клиента.

### 33-4 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

<b>interface INTERFACE-ID</b>	(Опционально) Укажите порт или диапазон портов для настройки.
<b>,</b>	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы



	до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Данная команда используется для отображения записей списка управления доступом (ACL) аппаратного порта на определенном интерфейсе в таблице оборудования.

**Пример**

В данном примере показано, как настроить отображение, когда включен DHCP Snooping в VLAN 100 – 110, интерфейс в режиме IP Source Filter Mode настроен как IP, существующая привязка произведена к порту 10.1.1.1 в VLAN 100.

```
Switch#show ip verify source interface ethernet 1/0/3
```

Interface	Filter-type	Filter-mode	IP address	MAC address	VLAN
eth1/0/3	ip	active	10.1.1.1	-	100
eth1/0/3	ip	active	deny-all	-	101-120

Total Entries: 2

```
Switch#
```

В данном примере показано, как настроить отображение, если интерфейс в режиме IP Source Filter Mode настроен как IP MAC, существующая привязка IP MAC привязывает IP-адрес 10.1.1.10 к MAC-адресу 00-01-01-01-01-01 в VLAN 100 и IP-адрес 10.1.1.11 к MAC-адресу 00-01-01-01-01-10 в VLAN 101.

```
Switch# show ip verify source interface eth1/0/3
```

Interface	Filter-type	Filter-mode	IP address	MAC address	VLAN
eth1/0/3	ip-mac	active	10.1.1.10	00-01-01-01-01-01	100
eth1/0/3	ip-mac	active	10.1.1.11	00-01-01-01-01-10	101
eth1/0/3	ip-mac	active	deny-all	-	102-120

Total Entries: 3

```
Switch#
```

**Отображаемые параметры**

<b>Interface</b>	Интерфейс, на котором включен IP Inspection.
------------------	--

<b>Filter-type</b>	Тип действующего IP Source Guard. <b>ip:</b> для авторизации IP-пакетов используется только IP-адрес. <b>ip-mac:</b> для авторизации IP-пакетов используется IP и MAC-адрес.
<b>Filter-Mode</b>	<b>Active:</b> активная проверка записей IP Source. <b>inactive-trust-port:</b> включить DHCP Snooping для доверенных портов без активной проверки записей IP Source. <b>inactive-no-snooping-vlan:</b> не настроено DHCP Snooping в VLAN, нет активной проверки записей IP Source.
<b>IP address</b>	IP-адрес клиента, назначенный DHCP-сервером или настроенный пользователем
<b>MAC address</b>	MAC-адрес клиента.
<b>VLAN</b>	Номер VLAN интерфейса клиента.

## 34. Команды IP Utility

### 34-1 ping

Данная команда используется для диагностики базового сетевого соединения.

```
ping {[ip] IP-ADDRESS | [ipv6] IPV6-ADDRESS | HOST-NAME} [count TIMES][timeout SECONDS] [source {IP ADDRESS | IPV6-ADDRESS}]
```

#### Параметры

<b>ip</b> <i>IP-ADDRESS</i>	(Опционально) Укажите, чтобы использовать IPv4-адрес. Укажите IPv4-адрес узла назначения (destination).
<b>ipv6</b> <i>IPV6-ADDRESS</i>	(Опционально) Укажите, чтобы использовать IPv6-адрес. Укажите IPv6-адрес системы, который необходимо обнаружить.
<i>HOST-NAME</i>	Укажите имя узла системы, которое необходимо обнаружить.
<b>count</b> <i>TIMES</i>	(Опционально) Укажите, чтобы завершить процесс после отправки указанного количества пакетов Echo Request.
<b>timeout</b> <i>SECONDS</i>	(Опционально) Укажите время ожидания ответа в секундах.
<b>source</b> { <i>IP ADDRESS   IPV6-ADDRESS</i> }	(Опционально) Укажите IP-адрес источника (source), используемый для пакетов команды Ping. Указанный IP-адрес должен быть одним из IP-адресов, сконфигурированных для коммутатора. У адреса назначения и IP-адреса источника должен быть один тип — IPv4 или IPv6.

#### По умолчанию

Значение **count** отключено. Пинг будет продолжаться до тех пор, пока пользователь не завершит процесс. Значение **timeout** составляет 1 секунду.

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте данную команду, чтобы проверить доступность, надежность и задержку маршрута к узлу назначения. Если не выбран параметр **count** или **timeout**, остановить Ping можно только используя комбинацию клавиш Ctrl+C.

#### Пример

В этом примере показано, как пинговать узел с IP-адресом 211.21.180.1 со счетом 4 раза.

```
Switch#ping 211.21.180.1 count 4

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

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

Switch#
```

В данном примере показано, как протестировать узел с IPv6-адресом 2001:238:f8a:77:7c10:41c0:6ddd:ecab.

```
Switch# ping 2001:238:f8a:77:7c10:41c0:6ddd:ecab

Reply from 2001:238:f8a:77:7c10:41c0:6ddd:ecab , bytes=100, time<10 ms
Reply from 2001:238:f8a:77:7c10:41c0:6ddd:ecab , bytes=100, time<10 ms
Reply from 2001:238:f8a:77:7c10:41c0:6ddd:ecab , bytes=100, time<10 ms
Reply from 2001:238:f8a:77:7c10:41c0:6ddd:ecab , bytes=100, time<10 ms

Ping Statistics for 2001:238:f8a:77:7c10:41c0:6ddd:ecab
Packets: Sent =4, Received =4, Lost =0

Switch#
```

## 34-2 ping access-class

Данная команда используется для указания списка доступа, который ограничит доступ для Ping. Используйте форму **no**, чтобы удалить проверку при помощи списка доступа.

```
ping access-class IP-ACL
no ping access-class
```

### Параметры

<i>IP-ACL</i>	Укажите стандартный список доступа IP. Поле адреса источника (source) разрешающей или запрещающей записи определяет, действителен узел, или нет.
---------------	--

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

Эта команда задает список доступа для ограничения доступа через ping. Для выполнения команды указанный список доступа не обязательно должен существовать.

### Пример

В этом примере показано, как создать ping access-class, который используется для ограничения ping только с узла 220.1.1.1 через стандартный список доступа IP.

```
Switch# configure terminal
Switch(config)# ip access-list ping-filter
Switch(config-ip-acl)# permit 220.1.1.1 255.255.255.255
Switch(config-ip-acl)# exit
Switch(config)# ping access-class ping-filter
Switch(config)#
```

## 35. Команды IPv6 Snooping

### 35-1 ipv6 snooping policy

Данная команда используется для создания или изменения политики IPv6 Snooping Policy. Команда позволяет войти в режим IPv6 Snooping Configuration Mode. При использовании формы **no** данная команда удаляет IPv6 Snooping Policy.

```
ipv6 snooping policy POLICY-NAME
no ipv6 snooping policy POLICY-NAME
```

#### Параметры

<i>POLICY-NAME</i>	Укажите имя политики IPv6 Snooping.
--------------------	-------------------------------------

#### По умолчанию

Политика IPv6 snooping не создается.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Данная команда используется для создания политики IPv6 Snooping Policy и входа в режим IPv6 Snooping Configuration Mode. После создания политики IPv6 Snooping используйте команду **ipv6 snooping attach-policy** для применения политики на указанном интерфейсе.

#### Пример

В данном примере показано, как создать политику IPv6 Snooping с именем policy1.

```
Switch# configure terminal
Switch(config)#ipv6 snooping policy policy1
Switch(config-ipv6-snooping)#
```

### 35-2 protocol

Данная команда используется для указания протокола, для которого необходимо применить IPv6 Snooping. При использовании формы **no** данная команда отключит IPv6 Snooping для указанного протокола.

```
protocol {dhcp | ndp}
no protocol {dhcp | ndp}
```

#### Параметры

<b>dhcp</b>	Укажите для отслеживания адресов DHCPv6-пакетов.
<b>ndp</b>	Укажите для отслеживания адресов NDP-пакетов.

#### По умолчанию

По умолчанию DHCPv6 и ND snooping отключены.

### Режим ввода команды

IPv6 Snooping Configuration Mode

### Использование команды

Функция Neighbor Discovery (ND) Snooping создана для автонастройки адресов IPv6 без аутентификации и адресов IPv6, настроенных вручную. Перед назначением адреса IPv6, узел должен сначала выполнить Duplicate Address Detection (DAD). ND Snooping обнаруживает сообщения DAD, включающие DAD Neighbor Solicitation (NS) и DAD Neighbor Advertisement (NA), для построения таблицы привязки. NDP-пакет (NS и NA) также используется для определения того, доступен ли узел по-прежнему и можно ли удалить привязку или нет.

DHCPv6 Snooping анализирует DHCPv6-пакеты, отправляемые между DHCPv6-клиентом и сервером во время процедуры назначения адреса. Когда DHCPv6-клиент успешно получает корректный IPv6-адрес, DHCPv6 Snooping создает его таблицу привязки.

DHCP-PD Snooping анализирует пакеты DHCPv6 Prefix Delegation (PD) между Delegating Router (назначенным IPv6-префиксом) и соответствующим Requesting Router для настройки привязки префикса.

### Пример

В данном примере показано, как включить DHCPv6 Snooping.

```
Switch# configure terminal
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# protocol dhcp
Switch(config-ipv6-snooping)#
```

## 35-3 limit address-count

Данная команда используется для ограничения максимального количества привязок IPv6 Snooping. При использовании формы **no** данная команда вернется в значения по умолчанию.

**limit address-count** *MAXIMUM*  
**no limit address-count**

### Параметры

<i>MAXIMUM</i>	Укажите максимальное количество привязок IPv6 Snooping. Доступен диапазон значений от 0 до 511.
----------------	--

### По умолчанию

По умолчанию лимит не настроен.

### Режим ввода команды

IPv6 Snooping Configuration Mode

**Использование команды**

Используйте эту команду для ограничения количества записей привязки IPv6, к которым применяется политика IPv6 snooping. Эта команда помогает ограничить размер таблицы привязки.

**Пример**

В этом примере показано, как ограничить количество записей привязки IPv6 snooping до 25.

```
Switch# configure terminal
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# limit address-count 25
Switch(config-ipv6-snooping)#
```

**35-4 ipv6 snooping attach-policy**

Данная команда используется для применения политики IPv6 Snooping Policy к указанной VLAN. При использовании формы **no** данная команда удалит привязку.

```
ipv6 snooping policy attach-policy POLICY-NAME
no ipv6 snooping policy attach-policy
```

**Параметры**

<i>POLICY-NAME</i>	Укажите имя политики IPv6 Snooping.
--------------------	-------------------------------------

**По умолчанию**

Нет

**Режим ввода команды**

VLAN Configuration Mode

**Использование команды**

Используйте эту команду для применения политики в определенной сети VLAN после создания политики IPv6 snooping.

**Пример**

В данном примере показано, как создать 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)#
```



## 35-5 ipv6 snooping station-move deny

Данная команда используется для запрета функции Station Move для привязки IPv6 Snooping. При использовании формы **no** данная команда вернется к значениям по умолчанию.

```
ipv6 snooping station-move deny
no ipv6 snooping station-move deny
```

### Параметры

Нет

### По умолчанию

По умолчанию функция Station Move разрешена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Когда функция Station Move разрешена, динамическая запись привязки Snooping с тем же VLAN ID и MAC-адресом на указанном порту может продвигаться 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)#
```

## 35-6 show ipv6 snooping policy

Данная команда используется для просмотра информации о DHCPv6 Guard.

```
show ipv6 snooping policy [POLICY-NAME]
```

### Параметры

<i>POLICY-NAME</i>	(Опционально) Укажите имя политики DHCPv6 Guard, которую необходимо отобразить.
--------------------	---

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте эту команду для отображения информации о защите DHCPv6. Если параметр не указан, будет отображена информация обо всех политиках.

### Пример

В этом примере показано, как отобразить информацию о защите DHCPv6.

```
Switch#show ipv6 snooping policy
```

```
Snooping policy: policyl
```

```
  Protocol: DHCP
```

```
  Limit Address Count: 25
```

```
  Target VLAN: 200
```

```
Switch#
```

## 36. Команды IPv6 Source Guard

### 36-1 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

<i>MAC-ADDRESS</i>	Укажите MAC-адрес привязки, созданной вручную.
<i>VLAN-ID</i>	Укажите VLAN привязки, созданной вручную.
<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес привязки, созданной вручную.
<i>INTERFACE-ID</i>	Укажите номер интерфейса привязки, созданной вручную.

#### По умолчанию

Нет

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Данная команда используется для добавления статической записи в таблицу привязки вручную. Для данной команды указанная VLAN необязательно должна существовать. Если указанный интерфейс позже будет удален, настройки команды будут соответственно также удалены.

#### Пример

В данном примере показано, как настроить привязку IPv6 Source Guard с адресом IPv6 2000::1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 на Ethernet 1/0/10.

```
Switch# configure terminal
Switch(config)# ipv6 source binding 00-01-02-03-04-05 vlan 2 2000::1 interface ethernet 1/0/1
Switch(config)#
```

### 36-2 ipv6 source-guard policy

Данная команда используется для создания политики IPv6 Source Guard Policy. Команда позволяет войти в режим IPv6 Source-Guard Policy Configuration Mode. При использовании формы **no** данная команда удалит политику IPv6 Source Guard Policy.

```
ipv6 source-guard policy POLICY-NAME
no ipv6 source-guard policy POLICY-NAME
```

#### Параметры

---

<i>POLICY-NAME</i>	Укажите имя политики IPv6 Source Guard Policy.
--------------------	--

---

**По умолчанию**

Нет

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Используйте эту команду для создания или удаления имени политики защиты источника. Эта команда вводит в режим конфигурации Source-guard Policy Configuration Mode.

**Пример**

В данном примере показано, как создать политику IPv6 Source Guard Policy.

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy policy1
Switch(config-source-guard)#
```

### 36-3 deny global-autoconfig

Данная команда используется для запрета автоматически сконфигурированного трафика. При использовании формы **no** команда отключит данную функцию.

**deny global-autoconfig**  
**no deny global-autoconfig**

**Параметры**

Нет

**По умолчанию**

По умолчанию данная опция разрешена.

**Режим ввода команды**

Source-Guard Policy Configuration Mode

**Использование команды**

Данная команда используется для запрета трафика от автоматически сконфигурированных глобальных адресов. Она может использоваться, когда все глобальные адреса назначены DHCP, и администратор хочет заблокировать входящий трафик от узлов с самостоятельно сконфигурированными адресами.

**Пример**

В данном примере показано, как запретить автоматически сконфигурированный трафик.

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy policy1
Switch(config-source-guard)# deny global-autoconfig
Switch(config-source-guard)#
```

### 36-4 permit link-local

Данная команда используется для аппаратного разрешения трафика данных, отправленного с адреса Link-Local. При использовании формы **no** команда отключит данную функцию.

**permit link-local**  
**no permit link-local**

#### Параметры

Нет

#### По умолчанию

По умолчанию этот параметр запрещен.

#### Режим ввода команды

Source-Guard Policy Configuration Mode

#### Использование команды

Используйте эту команду, чтобы включить или выключить аппаратное обеспечение для разрешения трафика данных, отправляемого по адресу link-local.

#### Пример

В данном примере показано, как разрешить весь трафик данных, отправленный с адреса Link-Local.

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy policy1
Switch(config-source-guard)# permit link-local
Switch(config-source-guard)#
```

### 36-5 ipv6 source-guard attach-policy

Данная команда используется для применения IPv6 Source Guard на интерфейсе. При использовании формы **no** данная команда удалит IPv6 Source Guard с интерфейса.

**ipv6 source-guard attach-policy [POLICY-NAME]**  
**no ipv6 source-guard attach-policy**

#### Параметры

---

*POLICY-NAME*

(Опционально) Укажите имя политики Source Guard Policy.

---

**По умолчанию**

Нет

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Когда команда применена к порту, принятый IPv6-пакет, кроме ND, RA, RS и DHCP-сообщений будет выполнять проверку привязки адреса. Пакет будет разрешен, если он соответствует любой записи в таблице привязки адресов. Таблица привязки включает в себя динамическую таблицу (созданную с помощью команд IPv6 Snooping) и статическую таблицу (созданную с помощью команды **ipv6 source binding vlan**).

Если имя политики не указано, по умолчанию политика Source Guard Policy разрешит пакеты, отправленные с помощью автоматически сконфигурированного адреса, и запретит пакеты, отправленные с адреса Link-Local.

**Пример**

В этом примере показано применение политики защиты источника IPv6 "pol1" к порту 3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ipv6 source-guard attach-policy pol1
Switch(config-if)#
```

**36-6 show ipv6 source-guard policy**

Данная команда используется для просмотра настроек IPv6 Source Guard Policy.

**show ipv6 source-guard policy [POLICY-NAME]**

**Параметры**

<i>POLICY-NAME</i>	(Опционально) Укажите имя политики Source Guard Policy.
--------------------	---

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Данная команда используется для просмотра настроек IPv6 Source Guard Policy. Если имя политики не указано, отображаться будет информация для всех политик IPv6 Source Guard.

**Пример**

В этом примере показано, как отобразить конфигурацию политики защиты источников IPv6.

```
Switch# show ipv6 dhcp guard policy
```

```
Policy Test configuration:
```

```
  permit link-local
```

```
  deny global-autoconf
```

```
  Target: eth1/0/3
```

```
Switch#
```

## 36-7 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

<b>vlan</b> <i>VLAN-ID</i>	(Опционально) Укажите для отображения привязок, соответствующих указанной VLAN.
<b>interface</b> <i>INTERFACE-ID</i>	(Опционально) Укажите для отображения привязок, соответствующих указанному номеру интерфейса.
<b>ipv6</b> <i>IPV6-ADDRESS</i>	(Опционально) Укажите для отображения привязок, соответствующих указанному адресу IPv6.
<b>mac</b> <i>MAC-ADDRESS</i>	(Опционально) Укажите для отображения привязок, соответствующих указанному MAC-адресу.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Команда используется для просмотра таблицы привязки.

### Пример

В данном примере показано, как включить отображение указанных записей из таблицы привязки.

```

Switch# show ipv6 neighbor binding

Codes: D - DHCPv6 Snooping, S - Static, N - ND Snooping
  IPv6 address          MAC address      Interface      VLAN Time left
N FE80::A8BB:CCFF:FE01:F500  AABB.CC01.F500 eth1/0/1       100  8850
S FE80::21D:71FF:FE99:4900   001D.7199.4900 eth1/0/1       100  N/A
N 2001:600::1             AABB.CC01.F500 eth1/0/2       100  3181
D 2001:300::1             AABB.CC01.F500 Port-channel3  100  9559
D 2001:100::2             AABB.CC01.F600 eth1/0/1       200  9196
D 2001:400::1             001D.7199.4900 eth1/0/2       100  1568
S 2001:500::1             000A.000B.000C eth1/0/13      300  N/A

Total Entries: 7

Switch#

```

### Отображаемые параметры

<b>Codes</b>	Коды для IPv6 Snooping Owner <b>D:</b> DHCPv6 Snooping <b>S:</b> Статический <b>N:</b> ND Snooping
<b>IPv6 address</b>	IPv6-адрес привязки.
<b>MAC address</b>	MAC-адрес привязки.
<b>Interface</b>	Номер интерфейса привязки.
<b>VLAN</b>	VLAN привязки.
<b>Time left</b>	Оставшееся время жизни привязки. Период отсутствия активности для статической привязки.

## 37. Команды Jumbo Frame

### 37-1 max-rcv-frame-size

Данная команда используется для настройки максимально допустимого размера Ethernet-фреймов. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```

max-rcv-frame-size BYTES
no max-rcv-frame-size

```

### Параметры

<b>BYTES</b>	Укажите максимально допустимый размер Ethernet-фреймов. Доступный диапазон значений: от 64 до 12288 байт.
--------------	--

### По умолчанию



Значение по умолчанию – 1536 байт.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Данная команда используется для конфигурирования физических портов. Фреймы избыточного размера будут отброшены, на входных портах будут проведены проверки. Используйте данную команду, чтобы передавать большие фреймы или jumbo-фреймы через коммутатор и оптимизировать передачу от сервера к серверу.

### Пример

В данном примере показано, как настроить максимальный размер полученных Ethernet-фреймов на порту 1/0/3. Указанное значение – 6000 байт.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/3
Switch(config-if)#max-rcv-frame-size 6000
Switch(config-if)#
```

## 38. Команды Link Aggregation Control Protocol (LACP)

### 38-1 channel-group

Данная команда используется для привязки интерфейса к агрегированной группе (channel-group). Используйте форму **no**, чтобы удалить интерфейс из агрегированной группы (channel-group).

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

#### Параметры

<i>CHANNEL-NO</i>	Укажите channel-group ID. Доступный диапазон значений: от 1 до 32.
<b>on</b>	Укажите интерфейс в качестве статического участника channel-group.
<b>active</b>	Укажите, чтобы включить для интерфейса режим LACP Active Mode.
<b>passive</b>	Укажите, чтобы включить для интерфейса режим LACP Passive Mode.

#### По умолчанию

Нет

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

Данная команда используется для конфигурирования физических портов. При первом подключении порта к channel-group система автоматически создаст port-channel. Интерфейс может подключиться только к одной channel-group.

Если в команде указан параметр **on**, тип channel-group – статическая. Если в команде указан параметр **active** или **passive**, тип channel-group – LACP. Channel-group может состоять только или из статических участников, или из участников LACP. После того как тип channel-group был определен, интерфейсы других типов не смогут подключиться к channel-group.

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

#### Пример

В этом примере показано, как назначить порты 4 и 5 в новую группу каналов LACP с идентификатором 3 и установить режим LACP на активный.

```
Switch# configure terminal
Switch(config)# interface range ethernet 1/0/4-1/0/5
Switch(config-if)# channel-group 3 mode active
Switch(config-if)#
```

## 38-2 lacp port-priority

Данная команда используется для настройки приоритета порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
lacp port-priority PRIORITY
no lacp port-priority
```

### Параметры

---

<i>PRIORITY</i>	Укажите приоритет порта в диапазоне от 1 до 65535.
-----------------	--

---

### По умолчанию

Приоритет порта по умолчанию – 32768.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Приоритет порта LACP определяет, какие порты могут подключиться к port-channel и на каких портах включен режим Standalone Mode. Чем ниже значение, тем выше приоритет. Если у двух и более портов совпадает приоритет, то приоритет будет определяться номером порта.

### Пример

В данном примере показано, как сконфигурировать приоритет порта на интерфейсах от Ethernet 1/0/4 до Ethernet 1/0/5. Указанное значение – 20000.

```
Switch# configure terminal
Switch(config)# interface range ethernet 1/0/4-1/0/5
Switch(config-if)# lacp port-priority 20000
Switch(config-if)#
```

## 38-3 lacp timeout

Данная команда используется для настройки таймера LACP Long или LACP Short. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
lacp timeout {short | long}
no lacp timeout
```

### Параметры

---

<b>short</b>	Укажите, чтобы выбрать значение 3 секунды для интервала,
--------------	--

---

	по истечении которого полученная информация о LACPDU будет объявлена недействительной, и 1 секунду для интервала между регулярными передачами LACP PDU. Данный параметр применяется, если канал-партнер использует Short Timeouts.
<b>long</b>	Укажите, чтобы выбрать значение 90 секунд для интервала, по истечении которого полученная информация о LACPDU будет объявлена недействительной, и 30 секунд для интервала между регулярными передачами LACP PDU. Данный параметр применяется, если канал-партнер использует Long Timeouts.

**По умолчанию**

Режим LACP Timeout по умолчанию – Short.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Используйте данную команду для конфигурирования физических портов.

**Пример**

В данном примере показано, как сконфигурировать режим LACP Timeout Long на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lacp timeout long
Switch(config-if)#
```

**38-4 lacp system-priority**

Данная команда используется для настройки приоритета системы. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
lacp system-priority PRIORITY
no lacp system-priority
```

**Параметры**

<i>PRIORITY</i>	Укажите приоритет системы в диапазоне от 1 до 65535.
-----------------	--

**По умолчанию**

Приоритет системы LACP по умолчанию – 32768.

**Режим ввода команды**

Global Configuration Mode

## Использование команды

Во время LACP-согласования локальный партнер обменивается с удаленным партнером приоритетом системы и приоритетом порта. При помощи приоритета порта коммутатор определяет, в каком режиме функционирует порт – Backup Mode или Active Mode. Приоритет системы LACP определяет коммутатор, контролирующий приоритет порта. Приоритеты портов других коммутаторов будут игнорированы.

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

## Пример

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

```
Switch# configure terminal
Switch(config)# lacp system-priority 30000
Switch(config)#
```

## 38-5 port-channel load-balance

Данная команда используется для настройки алгоритма Load Balancing (балансировка нагрузки), используемого коммутатором для распределения пакетов на порты одного канала. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}**  
**no port-channel load-balance**

## Параметры

<b>dst-ip</b>	Укажите, чтобы коммутатор проверил IP-адрес назначения (destination).
<b>dst-mac</b>	Укажите, чтобы коммутатор проверил MAC-адрес назначения.
<b>src-dst-ip</b>	Укажите, чтобы коммутатор проверил IP-адрес источника (source) и IP-адрес назначения.
<b>src-dst-mac</b>	Укажите, чтобы коммутатор проверил MAC-адрес источника и MAC-адрес назначения.
<b>src-ip</b>	Укажите, чтобы коммутатор проверил IP-адрес источника.
<b>src-mac</b>	Укажите, чтобы коммутатор проверил MAC-адрес источника.

## По умолчанию

Алгоритм Load Balancing по умолчанию – **src-dst-mac**.

## Режим ввода команды

Global Configuration Mode

## Использование команды

Используйте данную команду, чтобы указать алгоритм Load Balancing. Можно указать только один алгоритм.

### Пример

В данном примере показано, как сконфигурировать алгоритм Load Balancing src-ip.

```
Switch# configure terminal
Switch(config)# port-channel load-balance src-ip
Switch(config)#
```

## 38-6 show channel-group

Данная команда используется для отображения информации о channel-group.

**show channel-group [channel [CHANNEL-NO] {detail | neighbor} | load-balance | sys-id]**

### Параметры

<b>channel</b>	(Опционально) Укажите, чтобы отобразить информацию для указанных port-channel.
<i>CHANNEL-NO</i>	(Опционально) Укажите channel-group ID.
<b>detail</b>	(Опционально) Укажите, чтобы отобразить подробную информацию о channel-group.
<b>neighbor</b>	(Опционально) Укажите, чтобы отобразить информацию о соседнем устройстве.
<b>load-balance</b>	(Опционально) Укажите, чтобы отобразить информацию о балансировке нагрузки.
<b>sys-id</b>	(Опционально) Укажите, чтобы отобразить system identifier, используемый LACP.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Если номер канала порта не указан, будут отображены все каналы порта. Если в команде **show channel-group** параметр не указан, отображается краткая информация о группе каналов.

### Пример

В данном примере показано, как отобразить подробную информацию обо всех port-channel.

```

Switch# show channel-group channel detail

Flag:
  S - Port is requesting Slow LACPDU      F - Port is requesting fast LACPDU
  A - Port is in active mode              P - Port is in passive mode
LACP state:
  bundl:  Port is attached to an aggregator and bundled with other ports.
  hot-sby: Port is in a hot-standby state.
  indep:  Port is in an independent state(not bundled but able to switch data
          traffic)
  down:   Port is down.

Channel Group 1
Member Ports: 2, Maxports = 8, Protocol: LACP
Description:

```

Port	Flags	LACP State	Port Priority	Port Number
eth1/0/10	SA	bndl	32768	10
eth1/0/11	SA	bndl	32768	11

```

Channel Group 2
Member Ports: 2, Maxports = 8, Protocol: Static
Description:

```

Port	Flags	LACP State	Port Priority	Port Number
eth3/0/8	N/A	bndl	N/A	N/A
eth3/0/9	N/A	down	N/A	N/A

```

Switch#

```

В данном примере показано, как отобразить информацию о соседнем устройстве для port-channel 3.

```
Switch# show channel-group channel 3 neighbor

Flag:
 S - Port is requesting Slow LACPDU      F - Port is requesting fast LACPDU
 A - Port is in active mode              P - Port is in passive mode

Channel Group 3

```

Port	Partner System ID	Partner PortNo	Partner Flags	Partner Port_Pri
eth1/0/1	32768,F8-E9-80-1F-23-90	12	SP	32768
eth1/0/2	32768,F8-E9-80-1F-23-90	13	SP	32768

```
Switch#
```

В этом примере показано, как отобразить информацию о балансе нагрузки для всех групп каналов.

```
Switch# show channel-group load-balance

load-balance algorithm: src-dst-mac

Switch#

This example shows how to display the system identifier information.
Switch# show channel-group sys-id

System-ID: 32765,00-02-4B-29-3A-00

Switch#
```

В данном примере показано, как отобразить краткую информацию обо всех port-channel.

```
Switch# show channel-group

load-balance algorithm: src-dst-mac
System-ID: 32768,3C-1E-04-A1-CC-00

Group      Protocol
-----
1          LACP
2          Static

Switch#
```



## 39. Команды Link Layer Discovery Protocol (LLDP)

### 39-1 clear lldp counters

Данная команда используется для удаления статистики LLDP.

```
clear lldp counters [all | interface INTERFACE-ID [, | -]]
```

#### Параметры

<b>all</b>	(Опционально) Укажите, чтобы обнулить счетчик LLDP для всех интерфейсов и статистики Global LLDP.
<b>interface</b> INTERFACE-ID	(Опционально) Укажите интерфейс, на котором необходимо обнулить счетчик LLDP. Доступны только физические интерфейсы.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте данную команду, указав параметр **interface**, чтобы сбросить счетчик статистики LLDP на выбранном интерфейсе/интерфейсах. Используйте команду **clear lldp counters**, указав параметр **all**, чтобы удалить статистику LLDP и Global LLDP на всех интерфейсах. Если не указаны дополнительные параметры, будут обнулены только счетчики Global LLDP.

#### Пример

В данном примере показано, как удалить всю статистику LLDP.

```
Switch# clear lldp counters all
Switch#
```

### 39-2 clear lldp table

Данная команда используется для удаления всей информации об LLDP, полученной от соседних устройств.

```
clear lldp table {all | interface INTERFACE-ID [, | -]}
```

**Параметры**

<b>all</b>	Укажите, чтобы удалить информацию об LLDP, полученную от соседних устройств, для всех интерфейсов.
<i>INTERFACE-ID</i>	Укажите interface ID. Доступны только физические интерфейсы.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Если в команде не указан параметр **interface**, будет удалена вся информация, полученная от соседних устройств, на всех интерфейсах.

**Пример**

В данном примере показано, как удалить всю информацию, полученную от соседних устройств, на всех интерфейсах.

```
Switch# clear lldp table all
Switch#
```

**39-3 lldp dot1-tlv-select**

Данная команда используется для указания дополнительных настроек TLV (type-length-value) в указанном в пределах IEEE 802.1 наборе TLV, которые будут переданы и инкапсулированы в LLDPDU, а затем отправлены на соседние устройства. Используйте форму **no**, чтобы отключить передачу TLV.

```
lldp dot1-tlv-select {port-vlan | vlan-name [VLAN-ID [, | -]] | protocol-identity [PROTOCOL-NAME]}
no lldp dot1-tlv-select {port-vlan | vlan-name [VLAN-ID [, | -]] | protocol-identity [PROTOCOL-NAME]}
```

**Параметры**

<b>port-vlan</b>	Указывает TLV идентификатора VLAN порта для отправки. Port VLAN ID TLV - это дополнительный TLV фиксированной длины, который позволяет порту моста VLAN объявить идентификатор VLAN порта (PVID), который будет связан с нетегированными или приоритетно-тегированными кадрами.
------------------	---

<b>vlan-name</b>	Указывает TLV имени VLAN для отправки. TLV имени VLAN - это дополнительный TLV, который позволяет станции локальной сети IEEE 802.1Q, совместимой с IEEE 802, объявлять назначенное имя любой сети VLAN, с которой она настроена.
<i>VLAN-ID</i>	Указывает идентификатор VLAN в TLV имени VLAN. Диапазон идентификаторов VLAN ID составляет от 1 до 4094. Если идентификатор VLAN не указан, все настроенные VLAN для TLV имени VLAN будут очищены, и TLV имени VLAN не будет отправлен.
,	(Опционально) Указывает серию сетей VLAN или отделяет диапазон сетей VLAN от предыдущего диапазона. До или после запятой пробел не допускается.
-	(Опционально) Указывает диапазон сетей VLAN. До или после дефиса пробел не допускается.
<b>proto-col-identity</b>	Указывает TLV идентификации протокола для отправки. Protocol Identity TLV - это дополнительный TLV, который позволяет станции локальной сети IEEE 802 рекламировать определенные протоколы, доступные через порт.
<i>PROTOCOL-NAME</i>	(Опционально) Укажите имя протокола. Ниже перечислены допустимые для <i>PROTOCOL-NAME</i> строки: <b>eapol</b> - Extensible Authentication Protocol (EAP) over LAN <b>lacp</b> - Link Aggregation Control Protocol <b>gvrp</b> - GARP VLAN Registration Protocol <b>stp</b> - Spanning Tree Protocol

### По умолчанию

По умолчанию указанные в пределах IEEE 802.1 TLV не заданы.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Данная команда используется для конфигурирования физических портов. Если включено анонсирование дополнительных TLV, они будут инкапсулированы в LLDPDU и отправлены на другие устройства.

Тип Protocol Identity TLV определяет, анонсировать ли соответствующий экземпляр Protocol Identity локальной системы на порту. Protocol Identity TLV позволяет устройствам анонсировать протоколы, которые важны для работы сети. Например, такие протоколы как Spanning Tree Protocol, Link Aggregation Control Protocol и другие протоколы, установленные vendor-ом, отвечают за поддержку топологии и подключения к сети. Если работают обе функции протокола и на порту включено анонсирование Protocol Identity, Protocol Identity TLV будет анонсирован.

PPVID TLV будет отправлен на VLAN только при условии, что сконфигурированный VLAN ID соответствует настройкам Protocol VLAN на данном интерфейсе, а данная VLAN существует. VLAN будет анонсирована в VLAN Name TLV только при условии, что интерфейс является портом-членом сконфигурированного VLAN ID.

### Пример

В данном примере показано, как включить анонсирование Port VLAN ID TLV.

```
Switch#configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# lldp dot1-tlv-select port-vlan
Switch(config-if)#
```

В этом примере показано, как включить рекламу VLAN Name TLV с vlan1 на vlan3.

```
Switch# configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp dot1-tlv-select vlan-name 1-3
Switch(config-if)#
```

В этом примере показано, как включить рекламу TLV идентификации протокола LACP.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# lldp dot1-tlv-select protocol-identity lacp
Switch(config-if)#
```

### 39-4 lldp dot3-tlv-select

Данная команда используется для указания дополнительных настроек TLV в указанном в пределах IEEE 802.3 наборе TLV, которые будут инкапсулированы в LLDPDU, а затем отправлены на соседние устройства. Используйте форму **no**, чтобы отключить передачу TLV.

```
lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | power | max-frame-size]
no lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | power | max-frame-size]
```

#### Параметры

<b>mac-phy-cfg</b>	(Опционально) Укажите MAC/PHY Configuration/Status TLV, который необходимо отправить. MAC/PHY Configuration/Status TLV – это дополнительный TLV, который определяет (1) режим дуплекса и максимальную скорость передачи узла IEEE 802.3 LAN в бит/сек, а также (2) текущий режим дуплекса и настройки скорости передачи узла IEEE 802.3 LAN в бит/сек.
<b>link-aggregation</b>	(Опционально) Укажите Link Aggregation TLV, который необходимо отправить. Link Aggregation TLV содержит информацию о том, можно ли агрегировать группу, агрегируется ли группа в данный момент, а также информацию об агрегированном port channel ID. Если порт не агрегирован, значение port channel ID – 0.
<b>power</b>	(Необязательно) Указывает TLV питания через MDI для отправки. Три реализации IEEE 802.3 PMD (10BASE-T, 100BASE-TX и 1000BASE-T) позволяют подавать питание по

	каналу для подключенных систем без питания. Power Via MDI TLV позволяет сетевому управлению рекламировать и обнаруживать возможности поддержки питания MDI отправляющей станции локальной сети IEEE 802.3.
<b>max-frame-size</b>	(Опционально) Укажите Maximum Frame Size TLV, который необходимо отправить. Maximum Frame Size TLV указывает максимальный размер фрейма для используемого MAC и PHY.

**По умолчанию**

По умолчанию указанный в пределах IEEE 802.3 TLV не указан.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Эта команда доступна только для конфигурации интерфейса физического порта. Используйте эту команду для включения рекламы дополнительных TLV IEEE 802.3 Organizationally Specific. Соответствующий TLV будет инкапсулирован в LLDPDU и отправлен другим устройствам, если состояние рекламы включено.

**Пример**

В данном примере показано, как включить анонсирование MAC/PHY Configuration/Status TLV.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp dot3-tlv-select mac-phy-cfg
Switch(config-if)#
```

**39-5 lldp fast-count**

Данная команда используется для настройки количества отправляемых пакетов Fast Start (LLDP MED Fast Start Repeat Count Option) на коммутаторе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**lldp fast-count** *VALUE*  
**no lldp fast-count**

**Параметры**

<i>VALUE</i>	Укажите количество отправляемых пакетов Fast Start. Доступный диапазон значений: от 1 до 10.
--------------	---

**По умолчанию**

Значение по умолчанию – 4.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

При обнаружении LLDP MED Capabilities TLV будет запущена процедура Fast Start. Используйте данную команду, чтобы настроить количество отправляемых пакетов Fast Start, которое соответствует количеству передач LLDP-сообщений за один полный интервал Fast Start.

**Пример**

В этом примере показано, как настроить счетчик повторов быстрого запуска LLDP MED.

```
Switch# configure terminal
Switch(config)# lldp fast-count 10
Switch(config)#
```

**39-6 lldp hold-multiplier**

Данная команда используется для того, чтобы настроить множитель удержания для обновлений LLDP на коммутаторе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
lldp hold-multiplier VALUE
no hold-multiplier
```

**Параметры**

<i>VALUE</i>	Укажите множитель для интервала передачи LLDPDU, с помощью которого будет вычислено значение TTL для LLDPDU. Доступный диапазон значений: от 2 до 10.
--------------	---

**По умолчанию**

Значение по умолчанию – 4.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Данный параметр – это множитель для интервала передачи LLDPDU, с помощью которого будет вычислено значение TTL в LLDPDU. Время жизни определяется при помощи множителя удержания, умноженного на интервал TX. Если TTL для определенного анонса на соседнем коммутаторе истек, анонсированная информация будет удалена из MIB соседнего устройства.

**Пример**

В данном примере показано, как указать значение 3 для множителя удержания LLDP.

```
Switch# configure terminal
Switch(config)# lldp hold-multiplier 3
Switch(config)#
```

## 39-7 lldp management-address

Данная команда используется для настройки адреса управления (Management Address), который будет анонсирован на физическом интерфейсе. Используйте форму **no**, чтобы удалить заданные настройки.

**lldp management-address** [*IP-ADDRESS* | *IPV6-ADDRESS*]  
**no lldp management-address** [*IP-ADDRESS* | *IPV6-ADDRESS*]

### Параметры

<i>IP-ADDRESS</i>	(Опционально) Укажите IPv4-адрес, передаваемый в Management Address TLV.
<i>IPV6-ADDRESS</i>	(Опционально) Укажите IPv6-адрес, передаваемый в Management Address TLV.

### По умолчанию

По умолчанию адрес управления LLDP не настроен (Management Address TLV не отправляется).

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Данная команда используется для конфигурирования физических портов. Используйте данную команду, чтобы указать IPv4/IPv6-адрес, передаваемый в Management Address TLV на указанном порту. Если IP-адрес указан, но адрес не ассоциирован с одним из интерфейсов системы, адрес не будет отправлен.

Если при использовании команды **lldp management-address** не указан ни один адрес, коммутатор обнаружит по крайней мере один IPv4/IPv6-адрес в VLAN с самым низким VLAN ID. Если подходящих IPv4/IPv6-адресов нет, Management Address TLV анонсирован не будет. После того как администратор сконфигурировал адрес, оба адреса управления по умолчанию (IPv4 и IPv6) станут неактивны и не будут отправлены. IPv4/IPv6-адрес по умолчанию снова станет активен, если все сконфигурированные адреса будут удалены. Используйте данную команду несколько раз, чтобы создать несколько адресов управления IPv4/IPv6.

Используйте команду **no lldp management-address** без адреса управления, чтобы отключить адрес управления, анонсированный в LLDPDU. При отсутствии в списке действительного адреса управления, Management Address TLV отправлен не будет.

### Пример

В этом примере показано, как настроить IPv4-адрес управления на портах 1 - 3.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/1-3
Switch(config-if-range)# lldp management-address 10.1.1.1
Switch(config-if-range)#
```

В этом примере показано, как настроить IPv6-адрес управления на портах 4-6.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/4-6
Switch(config-if-range)# lldp management-address FE80::250:A2FF:FEBF:A056
Switch(config-if-range)#
```

В этом примере показано, как удалить управляющий IPv4-адрес с портов 1 - 3.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/1-3
Switch(config-if-range)# no lldp management-address 10.1.1.1
Switch(config-if-range)#
```

В этом примере показано, как удалить управляющий IPv6-адрес с портов 4-6.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/4-6
Switch(config-if-range)# no lldp management-address FE80::250:A2FF:FEBF:A056
Switch(config-if-range)#
```

В этом примере показано, как удалить все управляющие IPv4/IPv6-адреса с порта 5. С порта 5 не будет отправляться TLV адресов управления.

```
Switch# configure terminal
Switch(config)# interface eth1/0/5
Switch(config-if)# no lldp management-address
Switch(config-if)#
```

## 39-8 lldp med-tlv-select

Данная команда используется для указания дополнительного LLDP-MED TLV, который будет передан, инкапсулирован в LLDPDU и отправлен на соседние устройства. Используйте форму **no**, чтобы отключить передачу TLV.

```
lldp med-tlv-select [capabilities | inventory-management | network-policy | power-management]
no lldp med-tlv-select [capabilities | inventory-management | network-policy | power-management]
```

### Параметры

<b>capabilities</b>	(Опционально) Укажите, чтобы передать LLDP-MED Capabilities TLV.
<b>inventory-management</b>	(Опционально) Укажите, чтобы передать LLDP-MED Inventory Management TLV.
<b>network-policy</b>	(Опционально) Укажите, чтобы передать LLDP-MED Network Policy TLV.
<b>power- management</b>	(Опционально) Указывает передавать LLDP-MED расширенную мощность через MDI TLV, если локальное устройство является PSE-устройством или PD-устройством.



### По умолчанию

LLDP-MED TLV по умолчанию не выбран.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Используйте данную команду для конфигурирования физических портов. Команда применяется для включения/отключения передачи LLDP-MED TLV.

При отключении передачи Capabilities TLV будут также отключены LLDP-MED на физическом интерфейсе: LLDP-MED TLV не будут отправляться, даже если другие LLDP-MED TLV включены.

По умолчанию коммутатор отправляет LLDP-пакеты до тех пор, пока получает пакеты LLDP-MED от конечного устройства. Коммутатор отправляет пакеты LLDP-MED до тех пор, пока получает LLDP- пакеты.

### Пример

В данном примере показано, как включить передачу LLDP-MED TLV и LLDP-MED Capabilities TLV.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp med-tlv-select capabilities
Switch(config-if)#
```

## 39-9 lldp receive

Данная команда используется для того, чтобы включить на физическом интерфейсе получение LLDP-сообщений. Используйте форму **no**, чтобы отключить получение LLDP-сообщений.

**lldp receive**  
**no lldp receive**

### Параметры

Нет

### По умолчанию

По умолчанию функция LLDP включена на всех поддерживаемых интерфейсах.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Используйте данную команду для конфигурирования физических портов. Команда применяется для того, чтобы включить на интерфейсе получение LLDP-сообщений. Если LLDP не включен, коммутатор не будет получать LLDP-сообщения.

## Пример

В данном примере показано, как включить на физическом интерфейсе получение LLDP-сообщений.

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

## 39-10 lldp reinit

Данная команда используется для настройки минимального интервала перед повторной инициализацией на коммутаторе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**lldp reinit SECONDS**  
**no lldp reinit**

### Параметры

<i>SECONDS</i>	Укажите время задержки инициализации LLDP на интерфейсе. Доступный диапазон значений: от 1 до 10 секунд.
----------------	--

### По умолчанию

Значение по умолчанию – 2.

### Режим ввода команды

Global Configuration Mode

### Использование команды

При перезапуске физического интерфейса LLDP будет выдержан заданный интервал времени между последней командой **disable** и повторной инициализацией.

## Пример

В данном примере показано, как сконфигурировать интервал перед повторной инициализацией. Указанное значение – 5 секунд.

```
Switch# configure terminal
Switch(config)# lldp reinit 5
Switch(config)#
```

## 39-11 lldp run

Данная команда используется для глобального включения функции LLDP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**lldp run**  
**no lldp run**

## Параметры

Нет

## По умолчанию

По умолчанию данная опция отключена.

## Режим ввода команды

Global Configuration Mode

## Использование команды

Используйте данную команду, чтобы глобально включить функцию LLDP и инициировать передачу, получение и обработку LLDP-пакетов на коммутаторе. Используйте команду **lldp transmit**, чтобы контролировать передачу LLDP-пакетов, и команду **lldp receive**, чтобы контролировать получение LLDP-пакетов. Обе команды применяются в режиме Interface Configuration Mode. Для корректной работы на физическом интерфейсе необходимо включить LLDP как на физическом интерфейсе, так и глобально.

При анонсировании LLDP-пакетов коммутатор передает информацию соседним устройствам через физические интерфейсы. Коммутатор изучает информацию об управлении и возможности подключения, содержащуюся в LLDP-пакетах, анонсированных соседними устройствами.

## Пример

В данном примере показано, как включить функцию LLDP.

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

## 39-12 lldp forward

Данная команда используется для включения состояния LLDP Forwarding. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**lldp forward**  
**no lldp forward**

## Параметры

Нет

## По умолчанию

По умолчанию данная опция отключена.

## Режим ввода команды

Global Configuration Mode

## Использование команды

Данная функция глобально контролирует передачу LLDP. Если состояние LLDP Global отключено, а функция LLDP Forwarding включена, полученный LLDPDU-пакет будет передан.

### Пример

В данном примере показано, как включить состояние LLDP Forwarding глобально.

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

## 39-13 lldp tlv-select

Данная команда используется для выбора TLV в наборе 802.1AB Basic Management, а также для передачи TLV и его инкапсулирования в LLDPDU с последующей отправкой на соседние устройства. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**lldp tlv-select [port-description | system-capabilities | system-description | system-name]**  
**no lldp tlv-select [port-description | system-capabilities | system-description | system-name]**

### Параметры

<b>port-description</b>	(Опционально) Укажите Port Description TLV, который необходимо отправить. Port Description TLV позволяет анонсировать описание порта IEEE 802 LAN station.
<b>system-capabilities</b>	(Опционально) Укажите System Capabilities TLV, который необходимо отправить. Поле System Capabilities будет содержать bit-мар, определяющий основные функции системы.
<b>system-description</b>	(Опционально) Укажите System Description TLV, который необходимо отправить. System Description должно включать полное имя и версию аппаратного обеспечения, операционной системы и программного обеспечения.
<b>system-name</b>	(Опционально) Укажите System Name TLV, который необходимо отправить. System Name должно представлять собой полное имя домена системы.

### По умолчанию

По умолчанию дополнительный 802.1AB Basic Management TLV не указан.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Используйте данную команду для конфигурирования физических портов. Команда применяется для выбора дополнительных TLV, которые необходимо передать. Если выбрано анонсирование дополнительных TLV, они будут инкапсулированы в LLDPDU и отправлены на другие устройства.

## Пример

В данном примере показано, как включить все поддерживаемые дополнительные 802.1AB Basic Management TLV.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp tlv-select
Switch(config-if)#
```

В данном примере показано, как включить анонсирование System Name TLV.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp tlv-select system-name
Switch(config-if)#
```

## 39-14 lldp transmit

Данная команда используется для включения анонсирования/передачи LLDP. Используйте форму **no**, чтобы отключить передачу LLDP.

**lldp transmit**  
**no lldp transmit**

### Параметры

Нет

### По умолчанию

По умолчанию передача LLDP включена на всех поддерживаемых интерфейсах.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Используйте данную команду для конфигурирования физических портов. Команда применяется для включения передачи LLDP на физическом интерфейсе. Если LLDP не функционирует, коммутатор не будет передавать LLDP-сообщения.

## Пример

В данном примере показано, как включить передачу LLDP.

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

## 39-15 lldp tx-delay

Данная команда используется для настройки таймера Transmission Delay, определяющего минимальный интервал между отправкой LLDP-сообщений на основе постоянно изменяющегося содержания MIB. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
lldp tx-delay SECONDS
no lldp tx-delay
```

### Параметры

<i>SECONDS</i>	Укажите время задержки для отправки последовательных LLDPDU на интерфейсе. Доступный диапазон значений: от 1 до 8192 секунд, при этом указанное значение не должно превышать одну четвертую значения таймера Transmission Interval.
----------------	---

### По умолчанию

Значение по умолчанию – 2 секунды.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Значение LLDP Transmission Interval должно быть больше или равно значению таймера Transmission Delay, умноженному на четыре.

### Пример

В данном примере показано, как указать значение таймера Transmission Delay. Заданное значение – 8 секунд.

```
Switch# configure terminal
Switch(config)# lldp tx-delay 8
Switch(config)#
```

## 39-16 lldp tx-interval

Данная команда используется для настройки интервала LLDPDU Transmission. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
lldp tx-interval SECONDS
no lldp tx-interval
```

### Параметры

<i>SECONDS</i>	Укажите интервал между отправкой последовательных анонсов LLDPD на каждом физическом интерфейсе. Доступный диапазон значений: от 5 до 32768 секунд.
----------------	---

**По умолчанию**

Значение по умолчанию – 30 секунд.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Данный интервал определяет скорость передачи LLDP-пакетов.

**Пример**

В данном примере показано, как сконфигурировать отправку обновлений LLDP через каждые 50 секунд.

```
Switch# configure terminal
Switch(config)# lldp tx-interval 50
Switch(config)#
```

**39-17 snmp-server enable traps lldp**

Данная команда используется для включения отправки LLDP Trap и LLDP-MED Trap. Используйте форму **no**, чтобы отключить данную функцию.

```
snmp-server enable traps lldp [med]
no snmp-server enable traps lldp [med]
```

**Параметры**

<b>med</b>	(Опционально) Укажите, чтобы включить отправку LLDP-MED Trap.
------------	---

**По умолчанию**

По умолчанию отправка LLDP Trap и LLDP-MED Trap отключены.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Используйте команду **snmp-server enable traps lldp**, чтобы включить отправку LLDP-уведомлений. Используйте команду **snmp-server enable traps lldp med**, чтобы включить отправку LLDP-MED-уведомлений.

**Пример**

В данном примере показано, как включить отправку LLDP-MED Trap.

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

## 39-18 lldp notification enable

Данная команда используется для включения отправки уведомлений LLDP и LLDP-MED на интерфейсе. Используйте форму **no**, чтобы отключить данную функцию.

**lldp [med] notification enable**  
**no lldp [med] notification enable**

### Параметры

<b>med</b>	(Опционально) Укажите, чтобы включить уведомления LLDP-MED.
------------	---

### По умолчанию

По умолчанию уведомления LLDP и LLDP-MED отключены.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Используйте команду **lldp notification enable**, чтобы включить отставку уведомлений LLDP. Используйте команду **lldp med notification enable**, чтобы включить отставку уведомлений LLDP-MED.

### Пример

В данном примере показано, как включить отставку уведомлений LLDP-MED для интерфейса Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp med notification enable
Switch(config-if)#
```

## 39-19 lldp subtype

Данная команда используется для настройки подтипа LLDP TLV.

**lldp subtype port-id {mac-address | local}**

### Параметры

<b>port-id</b>	Укажите подтип Port ID TLV.
<b>mac-address</b>	Укажите, чтобы обозначить подтип Port ID TLV как «MAC Address (3)», а также чтобы закодировать MAC-адрес в поле «port ID».



<b>local</b>	Укажите, чтобы обозначить подтип Port ID TLV как «Locally assigned (7)», а также чтобы закодировать номер порта в поле «port ID».
--------------	---

**По умолчанию**

Подтип Port ID TLV по умолчанию – **local** (port number).

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Используйте данную команду, чтобы указать подтип LLDP TLV. Подтип Port ID указывает, как обозначен порт в поле port ID.

**Пример**

В данном примере показано, как сконфигурировать подтип Port ID TLV. Указанный подтип – mac-address.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp subtype port-id mac-address
Switch(config-if)#
```

**39-20 show lldp**

Данная команда используется для отображения общих настроек функции LLDP на коммутаторе.

**show lldp****Параметры**

Нет

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте данную команду, чтобы отобразить общие настройки функции LLDP на коммутаторе.

**Пример**

В этом примере показано, как отобразить глобальную конфигурацию LLDP коммутатора.

```

Switch#show lldp

LLDP System Information
  Chassis ID Subtype      : MAC Address
  Chassis ID              : F0-7D-68-12-50-01
  System Name             : Switch
  System Description      : Gigabit Ethernet Smart Managed Switch
  System Capabilities Supported: Repeater, Bridge
  System Capabilities Enabled  : Repeater, Bridge
LLDP-MED System Information:
  Device Class            : Network Connectivity Device
  Hardware Revision       : A1
  Software Revision       : 2.01.001
  Serial Number           : DGS1250102030
  Manufacturer Name      : D-Link Corporation
  Model Name              : DGS-1250-28XMP Gigabit Ethernet
  Asset ID                :
  PoE Device Type         : PSE Device
  PoE PSE Power Source    : Primary

LLDP Configurations
  LLDP State              : Disabled
  LLDP Forward State      : Disabled
  Message TX Interval     : 30
  Message TX Hold Multiplier: 4
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All

```

## 39-21 show lldp interface

Данная команда используется для того, чтобы отобразить настройки функции LLDP на физическом интерфейсе.

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

### Параметры

<i>INTERFACE-ID</i>	Укажите interface ID, который необходимо отобразить. Доступны только физические интерфейсы.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

### По умолчанию

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте данную команду, чтобы отобразить информацию о функции LLDP для каждого физического интерфейса.

**Пример**

В данном примере показано, как отобразить настройки функции LLDP для указанного физического интерфейса.

```

Switch# show lldp interface eth1/0/1

Port ID: eth1/0/1
-----
Port ID                               :eth1/0/1
Admin Status                           :TX and RX
Notification                            :Disabled
Basic Management TLVs:
  Port Description                       :Disabled
  System Name                            :Disabled
  System Description                     :Disabled
  System Capabilities                    :Disabled
  Enabled Management Address:
    (None)
IEEE 802.1 Organizationally Specific TLVs:
  Port VLAN ID                           :Disabled
  Enabled Port_and_Protocol_VLAN_ID
    (None)
  Enabled VLAN Name
    (None)
  Enabled Protocol_Identity
    (None)
IEEE 802.3 Organizationally Specific TLVs:
  MAC/PHY Configuration/Status           :Disabled
  Power Via MDI                           :Disabled
  Link Aggregation                        :Disabled
  Maximum Frame Size                      :Disabled
LLDP-MED Organizationally Specific TLVs:
  LLDP-MED Capabilities TLV               :Disabled
  LLDP-MED Network Policy TLV            :Disabled
  LLDP-MED Extended Power Via MDI PSE TLV :Disabled
  LLDP-MED Inventory TLV                 :Disabled

Switch#

```

**Отображаемые параметры****Enabled Management Address**

Отображает включенные IPv4/IPv6-адреса. «(None)» означает, что пользователь не сконфигурировал адрес управления (Management Address) при помощи команды

	<b>lldp management-address</b> или включенные IPv4/IPv6-адреса по умолчанию не применяются.
<b>Enabled Port and Protocol VLAN ID</b>	Отображает включенные Port and Protocol VLAN. В список VLAN включены сконфигурированные и включенные VLAN. При отсутствии сконфигурированных PPVID VLAN отображается «(None)».
<b>Enabled VLAN Name</b>	Отображает включенные VLAN для отправки VLAN Name TLV. В список VLAN включены сконфигурированные и включенные VLAN. При отсутствии сконфигурированных VLAN для VLAN Name TLV отображается «(None)».
<b>Enabled Protocol Identity</b>	Отображает включенную строку протокола для Protocol Identity TLV. При отсутствии включенных протоколов для Protocol Identity TLV отображается «(None)».

### 39-22 show lldp local interface

Данная команда используется для отображения информации о физическом интерфейсе, которая будет отправлена на соседние устройства в LLDP TLV.

**show lldp local interface** *INTERFACE-ID* [, | -] [**brief** | **detail**]

#### Параметры

<i>INTERFACE-ID</i>	Укажите interface ID. Доступны только физические интерфейсы.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
<b>brief</b>	(Опционально) Укажите, чтобы отобразить информацию в сокращенном формате.
<b>detail</b>	(Опционально) Укажите, чтобы отобразить информацию в подробном формате. Если не указан ни параметр <b>brief</b> , ни параметр <b>detail</b> , информация будет отображена в стандартном формате.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Эта команда доступна только для конфигурации интерфейса физического порта. Используйте эту команду для отображения локальной информации LLDP каждого физического интерфейса, доступной в настоящее время для заполнения исходящих объявлений LLDP.

**Пример**

В данном примере показано, как отобразить локальную информацию для интерфейса физического порта Ethernet 1/0/1 в подробном формате.

```
Switch#show lldp local interface ethernet 1/0/1 detail

Port ID: eth1/0/1
-----
Port ID Subtype           : Local
Port ID                   : eth1/0/1
Port Description          : D-Link Corporation DGS-1510-28XMP
                          HW A1 firmware 1.70.005 Port 1 on
                          Unit 1
Port PVID                  : 1
Management Address Count  : 2

  Address 1 : (default)
    Subtype           : IPv4
    Address           : 10.90.90.90
    IF Type           : IfIndex
    OID               : 1.3.6.1.4.1.171.10.137.9.1

  Address 2 :
    Subtype           : IPv4
    Address           : 10.90.90.90
    IF Type           : IfIndex
    OID               : 1.3.6.1.4.1.171.10.137.9.1

PPVID Entries Count      : 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

В данном примере показано, как отобразить локальную информацию для интерфейса физического порта Ethernet 1/0/1 в стандартном формате.

```

Switch#show lldp local interface ethernet 1/0/1

Port ID: eth1/0/1
-----
Port ID Subtype           : Local
Port ID                   : eth1/0/1
Port Description          : D-Link Corporation DGS-1510-28XMP
                           HW A1 firmware 1.70.005 Port 1 on
                           Unit 1
Port PVID                  : 1
Management Address Count  : 2
PPVID Entries Count       : 0
VLAN Name Entries Count   : 1
Protocol Identity Entries Count : 0
MAC/PHY Configuration/Status : (See Detail)
Power Via MDI              : (See Detail)
Link Aggregation          : (See Detail)
Maximum Frame Size        : 1536
LLDP-MED capabilities     : (See Detail)
Network Policy            : (See Detail)
Extended power via MDI    : (See Detail)

Switch#

```

В данном примере показано, как отобразить локальную информацию для интерфейса физического порта Ethernet 1/0/1 в кратком формате.

```

Switch#show lldp local interface ethernet 1/0/1 brief

Port ID: eth1/0/1
-----
Port ID Subtype           : Local
Port ID                   : eth1/0/1
Port Description          : D-Link Corporation DGS-1510-28XMP
                           HW A1 firmware 1.70.005 Port 1 on
                           Unit 1

Switch#

```

### 39-23 show lldp management-address

Данная команда используется для отображения информации об адресе управления (Management Address).

**show lldp management-address [IP-ADDRESS | IPV6-ADDRESS]****Параметры**

<i>IP-ADDRESS</i>	(Опционально) Укажите, чтобы отобразить информацию об LLDP Management для указанного IPv4-адреса.
<i>IPV6-ADDRESS</i>	(Опционально) Укажите, чтобы отобразить информацию об LLDP Management для указанного IPv6-адреса.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте данную команду, чтобы отобразить информацию об адресе управления.

**Пример**

В этом примере показано, как отобразить всю информацию об адресах управления.

```
Switch#show lldp management-address

Address 1 : (default)
-----
Subtype           : IPv4
Address           : 10.90.90.90
IF Type           : IfIndex
OID               : 1.3.6.1.4.1.171.10.165.2.1
Advertising Ports : -

Address 2 :
-----
Subtype           : IPv4
Address           : 10.90.90.90
IF Type           : IfIndex
OID               : 1.3.6.1.4.1.171.10.165.2.1
Advertising Ports : -

Total Entries : 2

Switch#
```



## 39-24 show lldp neighbor interface

Данная команда используется для отображения актуальной информации, полученной от соседнего устройства на указанном физическом интерфейсе.

**show lldp neighbors interface** *INTERFACE-ID* [, | -] [**brief** | **detail**]

### Параметры

<i>INTERFACE-ID</i>	Укажите interface ID. Доступны только физические интерфейсы.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
<b>brief</b>	(Опционально) Укажите, чтобы отобразить информацию в сокращенном формате.
<b>detail</b>	(Опционально) Укажите, чтобы отобразить информацию в подробном формате. Если не указан ни параметр <b>brief</b> , ни параметр <b>detail</b> , информация будет отображена в стандартном формате.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте данную команду, чтобы отобразить информацию, полученную от соседних устройств.

### Пример

В данном примере показано, как отобразить информацию о соседних устройствах, изученную LLDP на интерфейсе eth1/0/9, в подробном формате.

```
Switch#show lldp neighbors interface eth1/0/9 detail

Port ID: eth1/0/9
-----
Remote Entities Count : 1
Entity 1
  Chassis ID Subtype      : MAC Address
  Chassis ID              : F0-7D-68-30-36-00
  Port ID Subtype        : Local
  Port ID                 : eth1/0/10
  Port Description       :
  System Name            :
  System Description     :
  System Capabilities    :
  Management Address Count : 0
  (None)
  Port PVID              : 0
  PPVID Entries Count    : 0
  (None)
  VLAN Name Entries Count : 0
  (None)
  Protocol ID Entries Count : 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

В данном примере показано, как отобразить информацию о Remote LLDP в стандартном формате.

```
Switch#show lldp neighbors interface ethernet 1/0/9

Port ID: eth1/0/9
-----
Remote Entities Count : 1
Entity 1
  Chassis ID Subtype      : MAC Address
  Chassis ID              : F0-7D-68-30-36-00
  Port ID Subtype        : Local
  Port ID                 : eth1/0/10
  Port Description       :
  System Name            :
  System Description     :
  System Capabilities    :
  Management Address Count : 0
  Port PVID              : 0
  PPVID Entries Count    : 0
  VLAN Name Entries Count : 0
  Protocol ID Entries Count : 0
  MAC/PHY Configuration/Status : (None)
  Power Via MDI          : (None)
  Link Aggregation       : (None)
  Maximum Frame Size     : 0
  LLDP-MED capabilities  : (See Detail)
  Extended power via MDI : (See Detail)
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

В этом примере показано, как отобразить информацию о соседе на eth1/0/9 в кратком режиме.

```
Switch#show lldp neighbors interface ethernet 1/0/9 brief

Port ID: eth1/0/9
-----
Remote Entities Count : 1
Entity 1
  Chassis ID Subtype      : MAC Address
  Chassis ID              : F0-7D-68-30-36-00
  Port ID Subtype        : Local
  Port ID                 : eth1/0/10
  Port Description       :

Switch#
```

## 39-25 show lldp traffic

Данная команда используется для отображения глобальной информации о трафике LLDP.

```
show lldp traffic
```

### Параметры

Нет

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте данную команду, чтобы отобразить информацию об обнаружении соседних устройств на коммутаторе.

### Пример

В данном примере показано, как отобразить глобальную информацию о трафике LLDP.

```
Switch#show lldp traffic

Last Change Time   : 0D2H6M40S
Total Inserts      : 1
Total Deletes      : 0
Total Drops        : 0
Total Ageouts      : 0

Switch#
```

### Отображаемые параметры

<b>Last Change Time</b>	Время после последнего обновления до удаленной таблицы в днях, часах, минутах и секундах.
<b>Total Inserts</b>	Общее количество вставок в удаленную таблицу.
<b>Total Deletes</b>	Общее количество удалений из удаленной таблицы.
<b>Total Drops</b>	Общее количество случаев получения данных, которые не были добавлены в таблицу из-за непригодности.
<b>Total Ageouts</b>	Общее количество случаев удаления записей после истечения интервала Time to Live.

## 39-26 show lldp traffic interface

Данная команда используется для отображения информации о трафике LLDP на указанном физическом интерфейсе.

**show lldp traffic interface** *INTERFACE-ID* [, | -]

#### Параметры

<i>INTERFACE-ID</i>	Укажите interface ID. Доступны только физические интерфейсы.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте данную команду, чтобы отобразить трафик LLDP на каждом физическом интерфейсе.

#### Пример

В данном примере показано, как отобразить статистику для порта 1.

```
Switch#show lldp traffic interface ethernet 1/0/1
```

```
Port ID : eth1/0/1
```

```
-----
Total Transmits      : 0
Total Discards       : 0
Total Errors         : 0
Total Receives       : 0
Total TLV Discards   : 0
Total TLV Unknowns   : 0
Total Ageouts        : 0
```

```
Switch#
```

#### Отображаемые параметры

<b>Total Transmits</b>	Общее количество LLDP-пакетов, переданных на порту.
------------------------	---

<b>Total Discards</b>	Общее количество LLDP-кадров, отброшенных на порту.
<b>Total Errors</b>	Количество недействительных LLDP-кадров, полученных на порту.
<b>Total Receives</b>	Общее количество LLDP-пакетов, полученных на порту.
<b>Total TLV Discards</b>	Количество отброшенных TLV.
<b>Total TLV Unknowns</b>	Общее количество полученных на порту LLDP TLV, тип которых находится в зарезервированном диапазоне и не распознается.
<b>Total Ageouts</b>	Общее количество случаев удаления записей на порту после истечения интервала Time to Live.

## 40. Команды Loopback Detection (LBD)

### 40-1 loopback-detection (Global)

Данная команда используется для того, чтобы включить функцию LBD (Loopback Detection) глобально. Используйте форму **no**, чтобы глобально отключить данную функцию.

```
loopback-detection [mode {port-based | vlan-based}]
no loopback-detection [mode]
```

#### Параметры

<b>mode</b>	(Опционально) Укажите режим обнаружения.
<b>port-based</b>	Укажите режим обнаружения петли port-based (на порту).
<b>vlan-based</b>	Укажите режим обнаружения петли VLAN-based (в VLAN).

#### По умолчанию

По умолчанию данная опция отключена.  
Режим обнаружения по умолчанию – port-based.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Обычно режим port-based используется на портах, к которым подключены пользователи, а режим VLAN-based используется на trunk-портах и гибридных портах, если соседнее устройство не поддерживает функцию LBD.

Если включен режим port-based, порт, на котором включена функция LBD, будет отправлять нетегированные пакеты port-based LBD, чтобы обнаружить петлю. При наличии на пути петли передаваемый пакет вернется на тот же порт или на другой порт того же устройства. При обнаружении портом, на котором включена функция LBD, петли, на порту будет отключена передача и получение пакетов.

Если включен режим VLAN-based, порт будет периодически отправлять пакеты VLAN-based LBD на каждую VLAN, членом которой является данный порт, и на которой включена функция LBD. Если порт является тегированным членом VLAN, будут отправлены тегированные пакеты LBD. Если порт является нетегированным членом VLAN, будут отправлены нетегированные пакеты LBD. При наличии на пути VLAN петли, передача и получение пакетов будет временно остановлена на том порту закольцованной VLAN, где была обнаружена петля.

Если порт, на котором отключена функция LBD, получает пакет LBD и обнаруживает, что пакет отправлен системой, возможны два варианта: если тип данного пакета – port-based LBD, будет заблокирован порт отправления, а если тип пакета – VLAN-based LBD, будет заблокирована VLAN порта отправления.

Если на порту сконфигурирован режим VLAN-based, а порт является нетегированным членом нескольких VLAN, будет отправлен один нетегированный пакет LBD на каждую VLAN с указанием номера VLAN в поле VLAN пакета.

Восстановить порт, отключенный из-за ошибки, можно двумя способами: используйте команду **errdisable recovery cause loopback-detect**, чтобы включить автовосстановление, или восстановите порт вручную, применив сначала команду **shutdown**, а затем команду **no shutdown**.

Заблокированную VLAN можно восстановить автоматически, применив команду **errdisable recovery cause loopback-detect**. VLAN также можно восстановить вручную, применив сначала команду **shutdown**, а затем команду **no shutdown**.

### Пример

В данном примере показано, как включить функцию LBD глобально и установить режим обнаружения port-based.

```
Switch# configure terminal
Switch(config)# loopback-detection
Switch(config)# loopback-detection mode port-based
Switch(config)#
```

## 40-2 loopback-detection (Interface)

Данная команда используется для включения функции LBD на интерфейсе. Используйте форму **no**, чтобы отключить данную функцию на интерфейсе.

**loopback-detection**  
**no loopback-detection**

### Параметры

Нет

### По умолчанию

По умолчанию данная опция отключена.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Эта команда доступна только для конфигурации физического порта и интерфейса порт-канала. Используйте эту команду для включения или отключения функции обнаружения обратной петли на интерфейсе.

### Пример

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



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

### 40-3 loopback-detection interval

Данная команда используется для конфигурирования временного интервала. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**loopback-detection interval** *SECONDS*  
**no loopback-detection interval**

#### Параметры

<i>SECONDS</i>	Укажите интервал передачи пакетов LBD. Доступный диапазон значений: от 1 до 32767 секунд.
----------------	---

#### По умолчанию

По умолчанию это значение равно 10 секундам

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте эту команду для настройки интервала, с которым отправляются пакеты LBD для обнаружения возникновения связи.

#### Пример

В данном примере показано, как сконфигурировать интервал 20 секунд.

```
Switch# configure terminal
Switch(config)# loopback-detection interval 20
Switch(config)#
```

### 40-4 loopback-detection vlan

Данная команда используется для того, чтобы включить функцию LBD на VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**loopback-detection vlan** *VLAN-LIST*  
**no loopback-detection vlan** *VLAN-LIST*

#### Параметры

<i>VLAN-LIST</i>	Укажите идентификационный номер / номера / диапазон
------------------	---

---

номеров VLAN. Чтобы указать список диапазонов VLAN, введите одно или несколько значений, разделяя их при помощи запятых или дефисов.

---

### По умолчанию

По умолчанию данная опция включена для всех VLAN.

### Режим ввода команды

Global Configuration Mode

### Использование команд

Используйте данную команду, чтобы сконфигурировать список VLAN, на которых включена функция LBD. Настройки команды будут применены, если на порту сконфигурирован режим обнаружения петли VLAN-based.

По умолчанию пакеты LBD Control отправляются на все VLAN, членом которых является данный порт. Пакеты LBD Control отправляются на VLAN, членом которых является данный порт из указанного списка VLAN.

Список VLAN можно расширить, применив команду несколько раз.

### Пример

В данном примере показано, как включить функцию LBD в диапазоне с VLAN 100 по VLAN 200.

```
Switch# configure terminal
Switch(config)# loopback-detection vlan 100-200
Switch(config)#
```

## 40-5 show loopback-detection

Данная команда используется для отображения текущих настроек LBD.

**show loopback-detection [interface *INTERFACE-ID* [, | -]]**

### Параметры

<b>interface <i>INTERFACE-ID</i></b>	(Опционально) Укажите интерфейс, который необходимо отобразить.
<b>,</b>	(Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
<b>-</b>	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

### По умолчанию

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте данную команду, чтобы отобразить настройки и статус функции LBD.

**Пример**

В данном примере показано, как отобразить текущие настройки и статус функции LBD.

```
Switch# show loopback-detection

Loop Detection      : Enabled
Detection Mode     : port-based
LBD enabled VLAN   : all VLANs
Interval           : 10 seconds
Function Version    : v4.05

Interface          State      Result      Time Left (sec)
-----
eth1/0/1           Disabled  Normal      -
eth1/0/2           Disabled  Normal      -
eth1/0/3           Disabled  Normal      -
eth1/0/4           Disabled  Normal      -
eth1/0/5           Disabled  Normal      -
eth1/0/6           Disabled  Normal      -
eth1/0/7           Disabled  Normal      -
eth1/0/8           Disabled  Normal      -
eth1/0/9           Disabled  Normal      -
eth1/0/10          Disabled  Normal      -
eth1/0/11          Disabled  Normal      -
eth1/0/12          Disabled  Normal      -
eth1/0/13          Disabled  Normal      -

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

В данном примере показано, как отобразить статус функции LBD для интерфейса Ethernet 1/0/1.

```
Switch# show loopback-detection interface eth1/0/1

Interface          State      Result      Time Left (sec)
-----
eth1/0/1           Disabled  Normal      -

Switch#
```

**Отображаемые параметры**

<b>Interface</b>	Отображает порт, на котором включена функция LBD.
<b>State</b>	Отображает статус порта.
<b>Result</b>	Отображает, обнаружена ли петля.
<b>Time Left</b>	Отображает время, оставшееся до автовосстановления.

## 40-6 snmp-server enable traps loopback-detection

Данная команда используется для включения отправки SNMP-уведомлений для LBD. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**snmp-server enable traps loopback-detection**  
**no snmp-server enable traps loopback-detection**

### Параметры

Нет

### По умолчанию

По умолчанию данная функция отключена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте эту команду, чтобы включить или отключить отставку SNMP-уведомлений для обнаружения обратной связи.

### Пример

В данном примере показано, как включить отставку SNMP-уведомлений для LBD.

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

## 41. Команды Mirror

### 41-1 monitor session destination interface

Данная команда используется для того, чтобы настроить интерфейс назначения (destination) для сессии мониторинга, позволяя отслеживать пакеты на портах источника (source) через порт назначения. Используйте форму **no**, чтобы удалить интерфейс назначения сессии.

```
monitor session SESSION-NUMBER destination interface INTERFACE-ID
no monitor session SESSION-NUMBER destination interface INTERFACE-ID
no monitor session SESSION-NUMBER
```

#### Параметры

<i>SESSION-NUMBER</i>	Указывает номер сеанса для сеанса мониторинга порта. Допустимый номер - 1.
<i>INTERFACE-ID</i>	Указывает интерфейс назначения для сеанса мониторинга порта.

#### По умолчанию

Нет

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте эту команду для настройки интерфейса назначения для сеанса локального монитора.

В качестве интерфейсов назначения для сеансов мониторинга могут использоваться как физические порты, так и каналы портов. Для сеанса мониторинга можно указать несколько интерфейсов источника, но только один интерфейс назначения. Интерфейс не может быть одновременно интерфейсом источника одного сеанса и портом назначения другого сеанса. Интерфейс может быть настроен как интерфейс назначения нескольких сеансов, но может быть интерфейсом источника только одного сеанса.

#### Пример

В данном примере показано, как создать сессию мониторинга порта с номером 1, указав физический порт Ethernet 1/0/1 в качестве порта назначения, а три физических порта источника (от Ethernet 1/0/2 до Ethernet 1/0/4) в качестве портов источника.

```
Switch# configure terminal
Switch(config)# monitor session 1 destination interface eth1/0/1
Switch(config)# monitor session 1 source interface eth1/0/2-4
Switch(config)#
```

### 41-2 monitor session source interface

Данная команда используется для того, чтобы сконфигурировать порт источника (source) сессии мониторинга. Используйте форму **no**, чтобы удалить порт источника из сессии мониторинга.

**monitor session** *SESSION-NUMBER* **source interface** *INTERFACE-ID* [, | -] [**both** | **rx** | **tx**]  
**no monitor session** *SESSION-NUMBER* **source interface** *INTERFACE-ID* [, | -]  
**no monitor session** *SESSION-NUMBER*

#### Параметры

<i>SESSION-NUMBER</i>	Указывает номер сеанса для сеанса мониторинга порта. Допустимый номер - 1.
<b>interface</b> <i>INTERFACE-ID</i>	Укажите интерфейс источника для сессии мониторинга.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
<b>both</b>	(Опционально) Укажите, чтобы отслеживать пакеты, переданные и полученные портом.
<b>rx</b>	(Опционально) Укажите, чтобы отслеживать пакеты, полученные портом.
<b>tx</b>	(Опционально) Указывает для мониторинга пакетов, передаваемых на порту без переадресации, то есть независимо от статуса STG порта.

#### По умолчанию

Нет

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

В качестве исходных интерфейсов сеансов мониторинга могут использоваться как физические порты, так и каналы портов.

Для сеанса мониторинга можно указать несколько интерфейсов источника, но только один интерфейс назначения. Интерфейс не может быть одновременно интерфейсом источника одной сессии и портом назначения другой сессии. Интерфейс может быть настроен как интерфейс назначения нескольких сессий, но может быть интерфейсом источника только одной сессии.

Если направление не указано, отслеживается как TX (передаваемый), так и RX (принимаемый) трафик.

#### Пример

В данном примере показано, как создать сессию мониторинга порта с номером 1. Физический порт Ethernet 1/0/1 указан в качестве порта назначения, а три физических порта источника (от Ethernet 1/0/2 до Ethernet 1/0/4) указаны в качестве портов источника.

```
Switch# configure terminal
Switch(config)# monitor session 1 destination interface eth1/0/1
Switch(config)# monitor session 1 source interface eth1/0/2-4
Switch(config)#
```

### 41-3 show monitor session

Данная команда используется для отображения указанной сессии / всех сессий мониторинга.

**show monitor session** [*SESSION-NUMBER*]

#### Параметры

<i>SESSION-NUMBER</i>	(Опционально) Укажите номер сессии, которую необходимо отобразить. Значение равно – 1.
-----------------------	--

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте данную команду без указания номера сессии, чтобы отобразить все сессии мониторинга.

#### Пример

В данном примере показано, как отобразить сессию мониторинга порта с номером 1.

```
Switch# show monitor session 1
```

```
Session 1
```

```
Session Type: local session
```

```
Destination Port: Ethernet1/0/1
```

```
Source Ports:
```

```
Both:
```

```
Ethernet1/0/2
```

```
Ethernet1/0/3
```

```
Ethernet1/0/4
```

```
RX:
```

```
Ethernet1/0/5
```

```
TX:
```

```
Ethernet1/0/7
```

```
Total Entries: 1
```

```
Switch#
```



## 42. Команды Multicast Listener Discovery (MLD) Snooping

### 42-1 clear ipv6 mld snooping statistics

Данная команда используется для сброса счетчиков статистики MLD Snooping на коммутаторе.

```
clear ipv6 mld snooping statistics {all | vlan VLAN-ID | interface INTERFACE-ID}
```

#### Параметры

<b>all</b>	Укажите, чтобы очистить статистику IPv6 MLD Snooping для всех VLAN и портов.
<b>vlan VLAN-ID</b>	Укажите VLAN. Если VLAN не указана, будет очищена статистика всех VLAN.
<b>interface INTERFACE-ID</b>	Укажите интерфейс.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте данную команду, чтобы сбросить счетчики статистики MLD Snooping на коммутаторе.

#### Пример

В данном примере показано, как очистить всю статистику MLD Snooping.

```
Switch# clear ipv6 mld snooping statistics all
Switch#
```

### 42-2 ipv6 mld snooping

Данная команда используется для включения MLD Snooping. Используйте форму no, чтобы отключить MLD Snooping.

```
ipv6 mld snooping
no ipv6 mld snooping
```

#### Параметры

Нет

#### По умолчанию

Функция MLD Snooping отключена на всех VLAN интерфейсах.

Глобальное состояние MLD Snooping отключено.

#### Режим ввода команды

VLAN Configuration Mode  
Global Configuration Mode

#### Использование команды

Чтобы применить MLD Snooping на VLAN, необходимо включить глобальное состояние MLD Snooping и MLD Snooping на интерфейсе. Настройки IGMP Snooping и MLD Snooping являются независимыми, поэтому их можно включать одновременно на одной и той же VLAN.

#### Пример

В данном примере показано, как отключить MLD Snooping на всех VLAN.

```
Switch# configure terminal
Switch(config)# no ipv6 mld snooping
Switch(config)#
```

В данном примере показано, как включить MLD Snooping на VLAN, доступных для данной функции.

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping
Switch(config)#
```

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

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping
Switch(config-vlan)#
```

## 42-3 ipv6 mld snooping fast-leave

Данная команда используется для включения функции MLD Snooping Fast Leave на интерфейсе. Используйте форму **no**, чтобы отключить функцию MLD Snooping Fast Leave на интерфейсе.

**ipv6 mld snooping fast-leave**  
**no ipv6 mld snooping fast-leave**

#### Параметры

Нет

#### По умолчанию

По умолчанию данная опция отключена.

#### Режим ввода команды

VLAN Configuration Mode

## Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Используйте команду **ipv6 mld snooping fast-leave**, чтобы удалить принадлежность MLD с порта сразу же после получения сообщения Leave, не используя механизм запросов Group-Specific или Group-and-Source-Specific Query.

## Пример

В данном примере показано, как включить функцию MLD Snooping Fast Leave на VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping fast-leave
Switch(config-vlan)#
```

## 42-4 ipv6 mld snooping last-listener-query-interval

Данная команда используется для того, чтобы настроить интервал отправки сообщений Group-Specific или Group-and-Source-Specific (Channel) Query. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ipv6 mld snooping last-listener-query-interval SECONDS
no ipv6 mld snooping last-listener-query-interval
```

## Параметры

<i>SECONDS</i>	Укажите максимальный интервал между сообщениями Group-Specific Query. В том числе учитываются сообщения, отправленные в ответ на сообщения Leave Group. Доступный диапазон значений: от 1 до 25.
----------------	---

## По умолчанию

Значение по умолчанию – 1 секунда.

## Режим ввода команды

VLAN Configuration Mode

## Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Получив сообщение Done, MLD Snooping Querier считает, что на интерфейсе больше нет локальных участников, если после истечения времени ответа не пришло ни одно сообщение. Уменьшив данный интервал, можно сократить количество времени, которое требуется маршрутизатору для обнаружения потери последнего участника группы.

## Пример

В данном примере показано, как настроить интервал Last Listener Query. Указанное значение – 3 секунды.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping last-listener-query-interval 3
Switch(config-vlan)#
```

## 42-5 ipv6 mld snooping mrouter

Данная команда используется для того, чтобы настроить указанный интерфейс в качестве порта IPv6, подключенного к многоадресному маршрутизатору, или порта, которому запрещено подключаться к многоадресному маршрутизатору, на интерфейсе VLAN. Используйте форму **no**, чтобы удалить интерфейс из списка портов, подключенных к маршрутизатору, или портов, которым запрещено подключаться к многоадресному маршрутизатору.

```
ipv6 mld snooping mrouter {interface INTERFACE-ID [, | -] | forbidden interface INTERFACE-ID [, | -] |
learn pimv6}
no ipv6 mld snooping mrouter {interface INTERFACE-ID [, | -] | forbidden interface INTERFACE-ID [, | -]
| learn pimv6}
```

### Параметры

<b>interface</b>	Укажите диапазон интерфейсов, подключенных к многоадресным маршрутизаторам.
<b>forbidden interface</b>	Укажите диапазон интерфейсов, не подключенных к многоадресным маршрутизаторам.
<i>INTERFACE-ID</i>	Укажите интерфейс или список интерфейсов. Пробелы до и после запятой недопустимы. Доступны физические интерфейсы или port-channel.
,	(Опционально) Указывает серию интерфейсов или отделяет диапазон интерфейсов от предыдущего диапазона. До или после запятой пробел не допускается.
-	(Опционально) Указывает диапазон интерфейсов. До или после дефиса пробел не допускается.
<b>learn pimv6</b>	Укажите, чтобы включить динамическое изучение на портах, подключенных к многоадресному маршрутизатору.

### По умолчанию

Порт IPv6, подключенный к многоадресному маршрутизатору, не настроен.  
Автоматическое изучение включено.

### Режим ввода команды

VLAN Configuration Mode

### Использование команды

Чтобы указать порт маршрутизатора многоадресной рассылки, допустимым интерфейсом может быть физический порт или порт-канал. Указанный порт маршрутизатора многоадресной рассылки должен быть портом-членом сконфигурированной сети VLAN.

Порт многоадресного маршрутизатора может быть либо динамически обучаемым, либо статически настроенным на объект MLD snooping. При динамическом обучении устройство MLD snooping будет

прослушивать пакеты MLD и PIMv6, чтобы определить, является ли партнерское устройство маршрутизатором.

### Пример

В данном примере показано, как сконфигурировать интерфейс Ethernet 1/0/1 в качестве порта, подключенного к многоадресному маршрутизатору MLD Snooping, а интерфейс Ethernet 1/0/2 в качестве порта, не подключенного к многоадресному маршрутизатору MLD Snooping, на VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping mrouter interface ethernet 1/0/1
Switch(config-vlan)# ipv6 mld snooping mrouter forbidden interface ethernet 1/0/2
Switch(config-vlan)#
```

В данном примере показано, как отключить автоматическое изучение пакетов протокола маршрутизации.

```
Switch# configure terminal
Switch(config)# vlan 4
Switch(config-vlan)# no ipv6 mld snooping mrouter learn pimv6
Switch(config-vlan)#
```

## 42-6 ipv6 mld snooping querier

Данная команда используется для включения MLD Snooping Querier на коммутаторе. Используйте форму **no**, чтобы отключить MLD Snooping Querier.

```
ipv6 mld snooping querier
no ipv6 mld snooping querier
```

### Параметры

Нет

### По умолчанию

По умолчанию данная опция отключена.

### Режим ввода команды

VLAN Configuration Mode

### Использование команды

Если система может выполнить роль Querier, устройство будет анализировать пакеты MLD Query, отправленные другими устройствами. При получении сообщения MLD Query устройство с меньшим значением IPv6-адреса становится Querier. Если на интерфейсе также включен MLD-протокол, состояние MLD Snooping Querier будет отключено автоматически.

### Пример

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

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping querier
Switch(config-vlan)#
```

## 42-7 ipv6 mld snooping query-interval

Данная команда используется для того, чтобы задать интервал отправки сообщений MLD General Query. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**ipv6 mld snooping query-interval SECONDS**  
**no ipv6 mld snooping query-interval**

### Параметры

<i>SECONDS</i>	Укажите интервал между сообщениями MLD General Query, которые отправляет указанный маршрутизатор. Доступный диапазон значений: от 1 до 31744.
----------------	---

### По умолчанию

Значение по умолчанию – 125 секунд.

### Режим ввода команды

VLAN Configuration Mode

### Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Интервал MLD General Query – это промежуток времени между запросами General Query, отправляемыми Querier. Изменяя данный интервал, можно настроить количество сообщений MLD в сети. Чем больше значение интервала, тем реже будут отправляться сообщения MLD Query.

### Пример

В данном примере показано, как настроить интервал MLD Snooping Query на VLAN 1000. Указанное значение – 300 секунд.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping query-interval 300
Switch(config-vlan)#
```

## 42-8 ipv6 mld snooping query-max-response-time

Данная команда используется для настройки максимального времени ответа, анонсированного в запросах MLD Snooping Query. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**ipv6 mld snooping query-max-response-time SECONDS**  
**no ipv6 mld snooping query-max-response-time**

**Параметры**

<i>SECONDS</i>	Укажите максимальное время ответа, анонсированное в сообщениях MLD Snooping Query. Доступный диапазон значений: от 1 до 25 секунд.
----------------	--

**По умолчанию**

Значение по умолчанию – 10 секунд.

**Режим ввода команды**

VLAN Configuration Mode

**Использование команды**

Данная команда доступна только для конфигурирования интерфейса VLAN. Команда применяется для настройки периода времени, в течение которого участник группы может ответить на сообщение MLD Query. После истечения данного периода его участие в группе будет удалено.

**Пример**

В данном примере показано, как настроить максимальное время ответа на интерфейсе. Указанное значение – 20 секунд.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping query-max-response-time 20
Switch(config-vlan)#
```

**42-9 ipv6 mld snooping query-version**

Данная команда используется для того, чтобы настроить версию пакета General Query, отправленного MLD Snooping Querier. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**ipv6 mld snooping query-version {1 | 2}**  
**no ipv6 mld snooping query-version**

**Параметры**

<b>1</b>	Укажите версию пакета MLD General Query, отправленного MLD Snooping Querier – 1.
<b>2</b>	Укажите версию пакета MLD General Query, отправленного MLD Snooping Querier – 2.

**По умолчанию**

Версия по умолчанию – 2.

**Режим ввода команды**

VLAN Configuration Mode

### Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN.

### Пример

В данном примере показано, как указать версию Query на VLAN 1000. Указанная версия – 1.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping query-version 1
Switch(config-vlan)#
```

## 42-10 ipv6 mld snooping robustness-variable

Данная команда используется для настройки значения robustness variable для MLD Snooping. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**ipv6 mld snooping robustness-variable** *VALUE*  
**no ipv6 mld snooping robustness-variable**

### Параметры

<i>VALUE</i>	Укажите значение robustness variable в диапазоне от 1 до 7.
--------------	---

### По умолчанию

Значение по умолчанию – 2.

### Режим ввода команды

VLAN Configuration Mode

### Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN.

Robustness variable обеспечивает точную настройку в соответствии с ожидаемой потерей пакетов на интерфейсе. Значение robustness variable используется для вычисления следующих интервалов сообщений MLD:

- Group member interval – промежуток времени, по истечении которого маршрутизатор считает, что в группе больше нет активных участников. Данный интервал рассчитывается следующим образом: (robustness variable x query interval) + (1 x query response interval).
- Other querier present interval – промежуток времени, по истечении которого многоадресный маршрутизатор считает, что маршрутизатор, являющийся Querier, больше не доступен. Данный интервал рассчитывается следующим образом: (robustness variable x query interval) + (0,5 x query response interval).



- Last member query count – количество запросов Group-Specific Query, отправленных маршрутизатором до того, как он предполагает, что в группе нет локальных участников. Количество по умолчанию равно значению robustness variable.

Данное значение может быть увеличено, если в подсети ожидается потеря пакетов.

### Пример

В данном примере показано, как сконфигурировать значение robustness variable на интерфейсе VLAN 1000. Указанное значение – 3.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping robustness-variable 3
Switch(config-vlan)#
```

## 42-11 ipv6 mld snooping static-group

Данная команда используется для настройки статической группы MLD Snooping. Используйте форму **no**, чтобы удалить статическую группу.

**ipv6 mld snooping static-group** *IPV6-ADDRESS* **interface** *INTERFACE-ID* [, | -]  
**no ipv6 mld snooping static-group** *IPV6-ADDRESS* [**interface** *INTERFACE-ID* [, | -]]

### Параметры

<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес многоадресной группы.
<b>interface</b> <i>INTERFACE-ID</i>	Укажите интерфейс, который необходимо использовать.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

### По умолчанию

По умолчанию статическая группа не сконфигурирована.

### Режим ввода команды

VLAN Configuration Mode

### Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Используйте данную команду на интерфейсе VLAN, чтобы статически добавить записи об участии в группе и/или записи источника (source).

Используйте команду **ipv6 mld snooping static-group**, чтобы создать статическую группу MLD Snooping, если прикрепленный узел не поддерживает протокол MLD.

### Пример

В данном примере показано, как статически добавить группу и/или запись источника для MLD Snooping.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping static-group FF02::12:03 interface ethernet 1/0/5
Switch(config-vlan)#
```

## 42-12 ipv6 mld snooping minimum-version

Данная команда используется для настройки минимальной версии MLD, разрешенной на интерфейсе. Используйте форму **no**, чтобы удалить заданное ограничение.

**ipv6 mld snooping minimum-version 2**  
**no ipv6 mld snooping minimum-version**

### Параметры

Нет

### По умолчанию

По умолчанию ограничение не установлено.

### Режим ввода команды

VLAN Configuration Mode

### Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Данные настройки применимы только для фильтрации сообщений об участии MLD.

### Пример

В данном примере показано, как ограничить подключение всех узлов MLDv1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping minimum-version 2
Switch(config-vlan)#
```

## 42-13 show ipv6 mld snooping

Данная команда используется для отображения информации об MLD Snooping на коммутаторе.

**show ipv6 mld snooping [vlan VLAN-ID]**

### Параметры

---

**vlan VLAN-ID**

(Опционально) Укажите VLAN, которую необходимо отобразить.

---

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Если не указаны дополнительные параметры, будет отображена информация об MLD Snooping для всех VLAN, на которых включена данная функция.

### Пример

В данном примере показано, как отобразить настройки MLD Snooping.

```
Switch# show ipv6 mld snooping

MLD snooping global state: Enabled

VLAN #1 configuration
  MLD snooping state      : Enabled
  Minimum version         : v2
  Fast leave              : Enabled (host-based)
  Report suppression      : Enabled
  Suppression time        : 10 seconds
  Proxy reporting         : Disabled (Source ::)
  Mrouter port learning   : Enabled
  Querier state           : Enabled (Non-active)
  Query version           : v2
  Query interval          : 125 seconds
  Max response time       : 10 seconds
  Robustness value        : 2
  Last listener query interval : 1 seconds

Total Entries: 1

Switch#
```

## 42-14 show ipv6 mld snooping groups

Данная команда используется для отображения информации о группе MLD Snooping, изученной на коммутаторе.

```
show ipv6 mld snooping groups [IPV6-ADDRESS | vlan VLAN-ID]
```

**Параметры**

<i>IPV6-ADDRESS</i>	(Опционально) Укажите IP-адрес группы. Если IPv6-адрес не указан, будет отображена информация обо всех группах MLD Snooping.
<b>vlan</b> <i>VLAN-ID</i>	(Опционально) Укажите VLAN ID, который необходимо отобразить. Если VLAN не указана, будет отображена информация о группе MLD Snooping для всех VLAN.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

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

**Пример**

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

```
Switch# show ipv6 mld snooping groups

MLD Snooping Connected Group Membership:

VLAN ID  Group address      Source address      FM  Exp(sec)  Interface
-----  -
1         FF1E::              *                   EX  258       1/0/7
1         FF1E::3             *                   EX  258       1/0/7
1         FF1E::4             3620:110:1::3a2b   IN  258       1/0/7

Total Entries: 3

Switch#
```

**Отображаемые параметры**

<b>FM</b>	<b>Mode</b> (Режим фильтрации): Значение режима фильтрации может быть либо IN (Включить), либо EX (Исключить). EX - Режим фильтрации - Исключить. IN - Режим фильтрации - Включить.
<b>Exp (sec)</b>	<b>Expire time</b> (Время истечения): Время в секундах до истечения срока действия записи.

**42-15 show ipv6 mld snooping mrouter**

Данная команда используется для того, чтобы отобразить информацию об автоматически изученном или настроенном вручную многоадресном маршрутизаторе MLD Snooping.

**show ipv6 mld snooping mrouter [vlan VLAN-ID]**

#### Параметры

<b>vlan VLAN-ID</b>	(Опционально) Укажите VLAN ID, который необходимо отобразить. Если VLAN не указана, будет отображена информация о многоадресном маршрутизаторе MLD Snooping на всех VLAN.
---------------------	---

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте данную команду, чтобы отобразить интерфейсы динамически изученного или сконфигурированного вручную многоадресного маршрутизатора.

#### Пример

В данном примере показано, как отобразить информацию о многоадресном маршрутизаторе MLD Snooping.

```
Switch#show ipv6 mld snooping mrouter

VLAN  Ports
-----
1      1/0/3, 1/0/4 (static)
        1/0/6 (forbidden)
        1/0/7 (dynamic)

3      1/0/8 (static)
        1/0/9 (dynamic)

Total Entries: 2

Switch#
```

## 42- 16 show ipv6 mld snooping static-group

Данная команда используется для отображения статически сконфигурированных групп MLD Snooping на коммутаторе.

**show ipv6 mld snooping static-group [GROUP-ADDRESS | vlan VLAN-ID]**

**Параметры**

<i>GROUP-ADDRESS</i>	(Опционально) Укажите IPv6-адрес группы, который необходимо отобразить.
<b>vlan</b> <i>VLAN-ID</i>	(Опционально) Укажите VLAN ID, который необходимо отобразить.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Эта команда отображает информацию о статической группе MLD snooping.

**Пример**

В данном примере показано, как отобразить статически сконфигурированные группы MLD Snooping.

```
Switch#show ipv6 mld snooping static-group

VLAN ID  Group address                Interface
-----  -
1        FF1E::1                       1/0/1,1/0/5

Total Entries: 1

Switch#
```

**42- 17 show ipv6 mld snooping statistics**

Данная команда используется для отображения статистики MLD Snooping на коммутаторе.

**show ipv6 mld snooping statistics {interface [*INTERFACE-ID*] | vlan [*VLAN-ID*]}**

**Параметры**

<b>interface</b>	Укажите, чтобы отобразить счетчики статистики для интерфейса.
<i>INTERFACE-ID</i>	(Опционально) Укажите интерфейсы, которые необходимо отобразить.
<b>vlan</b>	Укажите, чтобы отобразить счетчики статистики для VLAN.
<i>VLAN-ID</i>	(Опционально) Укажите VLAN ID, который необходимо отобразить.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте данную команду, чтобы отобразить статистику MLD Snooping.

### Пример

В этом примере показано, как отобразить статистическую информацию MLD snooping на порту 4.

```
Switch# show ipv6 mld snooping statistics interface eth1/0/4

Interface eth1/0/4
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Total Entries: 1

Switch#
```

В этом примере показано, как отобразить статистическую информацию MLD snooping для VLAN 1.

```
Switch# show ipv6 mld snooping statistics vlan 1

VLAN 1 Statistics:
Rx: V1Report 3, v2Report 0, Query 3, v1Done 0
Tx: v1Report 2, v2Report 2, Query 1, v1Done 2

Total Entries: 1

Switch#
```

## 43. Команды Multiple Spanning Tree Protocol (MSTP)

### 43-1 instance

Данная команда используется для привязки VLAN к MST-экземпляру. Для удаления экземпляров без указания VLAN воспользуйтесь командой **no instance**. Для возврата привязки VLAN к экземпляру по умолчанию (CIST) воспользуйтесь командой **no instance**.

```
instance INSTANCE-ID vlans VLAN-ID [, | -]
no instance INSTANCE-ID [vlans VLAN-ID [, | -]]
```

#### Параметры

<b>vlan</b> VLAN-ID	Укажите VLAN, которые необходимо привязать или удалить из указанного экземпляра. Доступный диапазон значений: от 1 до 4094.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
INSTANCE-ID	Указывает идентификатор экземпляра MSTP, к которому привязаны указанные сети VLAN. Это значение должно быть в диапазоне от 1 до 32.

#### По умолчанию

Нет

#### Режим ввода команды

MST Configuration Mode

#### Использование команды

Любая непривязанная VLAN привязывается к экземпляру CIST. Во время привязки VLAN к несуществующему экземпляру, экземпляр будет создан автоматически. Если все VLAN экземпляра удалены, экземпляр будет удален автоматически. Пользователи могут удалить экземпляр вручную, используя команду **no instance** без указания VLAN.

#### Пример

В данном примере показано, как привязать несколько VLAN к экземпляру 2.

```
Switch# configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)# instance 2 vlans 1-100
Switch(config-mst)#
```

### 43-2 name



Данная команда используется для настройки имени MST-региона. Используйте форму `no`, чтобы вернуться к настройкам по умолчанию. Для возврата к настройкам по умолчанию воспользуйтесь формой `no`.

**name** *NAME*  
**no name** *NAME*

#### Параметры

<i>NAME</i>	Определяет имя, заданное для указанного региона MST. Строка имени имеет максимальную длину 32 символа, а тип - общая строка, допускающая пробелы.
-------------	---

#### По умолчанию

Имя по умолчанию – MAC-адрес коммутатора.

#### Режим ввода команды

MST Configuration Mode

#### Использование команды

Если у коммутаторов совпадают VLAN Mapping и номер версии конфигурации, но различаются имена регионов, они принадлежат к разным MST-регионам.

#### Пример

В данном примере показано, как настроить имя MSTP. Настроенное имя – MName.

```
Switch# configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)# name MName
Switch(config-mst)#
```

### 43-3 revision

Данная команда используется для настройки номера ревизии для MST. Для возврата к настройкам по умолчанию воспользуйтесь формой `no`.

**revision** *VERSION*  
**no revision**

#### Параметры

<i>VERSION</i>	Укажите номер ревизии для MST. Доступный диапазон значений: от 0 до 65535.
----------------	--

#### По умолчанию

Значение по умолчанию – 0.

#### Режим ввода команды

## MST Configuration Mode

## Использование команды

Два коммутатора Ethernet с идентичной конфигурацией принадлежат к разным регионам, если их номера ревизии не совпадают.

## Пример

В данном примере показано, как настроить revision level MSTP. Настроенное значение – 2.

```
Switch# configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)# revision 2
Switch(config-mst)#
```

## 43-4 show spanning-tree mst

Данная команда используется для отображения информации, которая использовалась в версии MSTP.

```
show spanning-tree mst [configuration [digest]]
show spanning-tree mst [instance INSTANCE-ID [, | -]] [interface INTERFACE-ID [, | -]] [detail]
```

## Параметры

<b>configuration</b>	(Опционально) Указывает конфигурацию MST оборудования.
<b>digest</b>	(Опционально) Указывает отображение дайджеста MD5, включенного в текущий идентификатор конфигурации MST (MSTCI).
<b>instance</b> <i>INSTANCE-ID</i> [,   -]	(Опционально) Укажите номер экземпляра, который будет отображаться.
,	(Опционально) Указывает серию экземпляров или отделяет диапазон экземпляров от предыдущего диапазона. До или после запятой пробел не допускается.
-	(Опционально) Указывает диапазон экземпляров. До или после дефиса пробел не допускается.
<b>interface</b> <i>INTERFACE-ID</i>	(Опционально) Укажите идентификатор интерфейса, который будет отображаться.
,	(Опционально) Указывает серию интерфейсов или отделяет диапазон интерфейсов от предыдущего диапазона. До или после запятой пробел не допускается.
-	(Опционально) Указывает диапазон интерфейсов. До или после дефиса пробел не допускается.

## По умолчанию

Нет

## Режим ввода команды

EXEC Mode

**Использование команды**

Используйте данную команду для отображения настроек и рабочего состояния MSTP. Если настроена Private VLAN, а второстепенная (Secondary) VLAN не привязана к той же основной (Primary) VLAN, команда **show spanning-tree mst configuration** отобразит сообщение, указывающее на это условие.

**Пример**

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

```
Switch#show spanning-tree mst detail

Spanning tree: Enabled,protocol: MSTP
Number of MST instances: 1

>>>MST00 vlans mapped : 1-4094
Bridge Address: 00-01-02-03-04-11, Priority: 32768 (32768 sysid 0)
Designated Root Address: 00-00-AB-CD-12-34, Priority: 32768 (32768 sysid 0)
Regional Root Bridge Address: 00-01-02-03-04-11, Priority: 32768 (32768 sysid 0)
Designated Bridge Address: 00-00-AB-CD-12-34, Priority: 32768 (32768 sysid 0)
Topology Changes Count: 5

eth1/0/1
  Port state: forwarding
  Port role: root
  Port info : port ID 128.1, priority: 128, cost: 20000
  Designated root address: 00-00-AB-CD-12-34, priority: 32768
  Regional Root address: 00-00-AB-CD-12-34, priority: 32768
  Designated bridge address: 00-00-AB-CD-12-34, priority: 32768, port id: 128.1

eth1/0/2
  Port state: blocking
  Port role: alternate
  Port info : port ID 128.2, priority: 128, cost: 20000
  Designated root address: 00-00-AB-CD-12-34, priority: 32768
  Regional Root address: 00-00-AB-CD-12-34, priority: 32768
  Designated bridge address: 00-00-AB-CD-12-34, priority: 32768, port id: 128.2

Switch#
```

В данном примере показано, как отобразить подробную информацию об MSTP для интерфейса eth1/0/1.

```
Switch#show spanning-tree mst interface eth 1/0/1 detail

eth1/0/1
  Configured link type: auto, operation status: point-to-point
  Configured fast-forwarding: auto, operation status: non-edge

>>>>MST instance: 00, vlans mapped : 1-4094
  Port state: forwarding
  Port role: nonStp
  Port info : port ID 128.1, priority: 128, cost: 200000
  Designated root address: 00-00-00-00-00-00, priority: 0
  Regional Root address: 00-00-00-00-00-00, priority: 0
  Designated bridge address: 00-00-00-00-00-00, priority: 0, port id: 0.0

Switch#
```

В данном примере показано, как отобразить краткую информацию об MSTP.

```
Switch# show spanning-tree mst

Spanning tree: Enabled,protocol: MSTP
Number of MST instances: 1

>>>>MST00 vlans mapped : 1-4094
Bridge Address: 00-01-02-03-04-11, Priority: 32768 (32768 sysid 0)
Designated Root Address: 00-00-AB-CD-12-34, Priority: 32768 (32768 sysid 0)
Regional Root Bridge Address: 00-01-02-03-04-11, Priority: 32768 (32768 sysid 0)
Designated Bridge Address: 00-00-AB-CD-12-34, Priority: 32768 (32768 sysid 0)
Topology Changes Count: 5

Interface      Role      State      Cost      Priority Link
-----      -
eth1/0/1      root      forwarding 20000     128.1    p2p      non-edge
eth1/0/2      alternate blocking 20000     128.2    p2p      non-edge

Switch#
```

В данном примере показано, как отобразить краткую информацию об MSTP для интерфейсов от eth1/0/3 до eth1/0/4.

```
Switch# show spanning-tree mst interface eth 1/0/3-4

eth1/0/3
Configured link type: auto, operation status: point-to-point
Configured fast-forwarding: auto, operation status: edge

Instance  Role      State      Cost      Priority
-----  ----  -----  -
MST00    designated forwarding  20000    128.3
MST01    backup   blocking   200000    128.3

eth1/0/4
Configured link type: auto, operation status: point-to-point
Configured fast-forwarding: auto, operation status: edge

Instance  Role      State      Cost      Priority
-----  ----  -----  -
MST00    root     forwarding 20000    128.4
MST01    backup   blocking   200000    128.4

Switch#
```

В данном примере показано, как отобразить краткую информацию об MSTP для интерфейсов от eth1/0/3 до eth1/0/4 MST02.

```
Switch# show spanning-tree mst instance 2 interface eth 1/0/3-4

>>>>MST02 vlans mapped: 2-3
Bridge Address:00-12-d9-87-47-00 , Priority: 32770 (32768 sysid 2)
Designated Root Address:00-12-d9-87-47-00 , Priority: 32770
Designated Bridge Address:00-12-d9-87-47-00 , Priority: 32770

Interface  Role      State      Cost      Priority
-----  ----  -----  -
eth1/0/3   backup   blocking   200000    128.3
eth1/0/4   backup   blocking   200000    128.4

Switch#
```

В данном примере показано, как отобразить настройки привязки экземпляра MSTP.

```
Switch# show spanning-tree mst configuration
```

```
Name      : [region1]
Revision  : 2, Instances configured: 3
Digest    : A222086F87562346CA7D40AD90AB61ED
Instance  Vlans
-----  -----
0         21-4094
1         1-10
2         11-20

Switch#
```

## 43-5 spanning-tree mst

Данная команда используется для настройки параметров стоимости пути и приоритета порта для MST-экземпляра (включая CIST с ID экземпляра 0). Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

```
spanning-tree mst INSTANCE-ID {cost COST | port-priority PRIORITY}
no spanning-tree mst INSTANCE-ID {cost | port-priority}
```

### Параметры

<b>instance</b> <i>INTANCE-ID</i>	Укажите номер экземпляра.
<b>cost</b> <i>COST</i>	Укажите стоимость пути экземпляра. Доступный диапазон значений: от 0 до 200000000.
<b>port-priority</b> <i>PRIORITY</i>	Укажите приоритет порта экземпляра. диапазон значений: от 0 до 240 с шагом 16.

### По умолчанию

Стоимость зависит от скорости порта. Чем выше скорость интерфейса, тем меньше стоимость. MST всегда использует стоимость длинного пути.

Приоритет порта по умолчанию – 128.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

При вводе стоимости запятая в записи не ставится. Например, 1000, а не 1,000.

### Пример

В данном примере показано, как настроить стоимость пути интерфейса.

```
Switch# configure terminal
Switch(config)#interface eth 1/0/1
Switch(config-if)# spanning-tree mst 0 cost 17031970
Switch(config-if)#
```

## 43-6 spanning-tree mst configuration

Данная команда используется для входа в режим MST Configuration. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

**spanning-tree mst configuration**  
**no spanning-tree mst configuration**

### Параметры

Нет

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

Данная команда используется для входа в режим MST Configuration.

### Пример

В данном примере показано, как войти в режим MST Configuration.

```
Switch# configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#
```

## 43-7 spanning-tree mst max-hops

Данная команда используется для настройки максимального числа переходов MSTP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

**spanning-tree mst max-hops HOP-COUNT**  
**no spanning-tree mst max-hops**

### Параметры

<b>max-hops HOP-COUNT</b>	Указывает максимальное число хопов MSTP. Диапазон составляет от 6 до 40 переходов.
---------------------------	--

### По умолчанию

Значение по умолчанию – 20 переходов.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду, чтобы настроить максимальное число переходов MSTP.

### Пример

В данном примере показано, как настроить максимальное число переходов MSTP.

```
Switch# configure terminal
Switch(config)#spanning-tree mst max-hops 19
Switch(config)#
```

## 43-8 spanning-tree mst hello-time

Данная команда используется для настройки параметра Hello Time в версии MSTP для каждого порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

**spanning-tree mst hello-time SECONDS**  
**no spanning-tree mst hello-time**

### Параметры

<i>SECONDS</i>	Укажите интервал между отправкой одного BPDU-сообщения для назначенного порта (Designated Port). Доступный диапазон значений: от 1 до 2 секунд.
----------------	--

### По умолчанию

Значение параметра Hello Time по умолчанию – 2 секунды.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Команда применима только в режиме MSTP.

### Пример

В данном примере показано, как настроить параметр Hello Time в версии MSTP для интерфейса Ethernet 1/0/1. Указанное значение – 1 секунда.

```
Switch# configure terminal
Switch(config)#interface eth 1/0/1
Switch(config-if)# spanning-tree mst hello-time 1
Switch(config-if)#
```

## 43-9 spanning-tree mst priority

Данная команда используется для настройки значения приоритета моста для выбранного MSTP-экземпляра. Для возврата к настройкам по умолчанию воспользуйтесь формой **no**.

**spanning-tree mst INSTANCE-ID priority PRIORITY**



**no spanning-tree mst INSTANCE-ID priority****Параметры**

<i>INSTANCE-ID</i>	Укажите ID MSTP-экземпляра. По умолчанию значение экземпляра CIST равно 0.
<i>PRIORITY</i>	Укажите приоритет моста, значение которого должно делиться на 4096. Доступный диапазон значений: от 0 до 61440.

**По умолчанию**

Значение по умолчанию – 32768.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Приоритет имеет то же значение, что и приоритет моста в справочнике команд STP, но может указывать другой приоритет для разных MSTP-экземпляров.

**Пример**

В данном примере показано, как настроить приоритет моста для MSTP-экземпляра 2.

```
Switch# configure terminal
Switch(config)#spanning-tree mst 2 priority 0
Switch(config)#
```

## 44. Команды Neighbor Discovery (ND) Inspection

### 44-1 ipv6 nd inspection policy

Данная команда используется для создания политики ND Inspection Policy и для входа в режим ND Inspection Policy Configuration Mode. Используйте форму **no**, чтобы удалить политику ND Inspection Policy.

```
ipv6 nd inspection policy POLICY-NAME
no ipv6 nd inspection policy POLICY-NAME
```

#### Параметры

<i>POLICY-NAME</i>	Укажите имя политики ND Inspection Policy.
--------------------	--

#### По умолчанию

Нет

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте данную команду, чтобы создать политику ND Inspection Policy и войти в режим ND Inspection Policy Configuration Mode. ND Inspection предназначена для проверки сообщений Neighbor Solicitation (NS) и Neighbor Advertisement (NA).

#### Пример

В данном примере показано, как создать политику ND под именем «policy1».

```
Switch# configure terminal
Switch(config)# ipv6 nd inspection policy policy1
Switch(config-nd-inspection)#
```

### 44-2 validate source-mac

Данная команда используется для проверки MAC-адреса на соответствие адресу Link Layer для ND-сообщений. Используйте форму **no**, чтобы отменить проверку.

```
validate source-mac
no validate source-mac
```

#### Параметры

Нет

#### По умолчанию

По умолчанию данная функция отключена.

**Режим ввода команды**

ND Inspection Policy Configuration Mode

**Использование команды**

Когда коммутатор получит ND-сообщение, содержащее адрес Link Layer, исходный MAC-адрес будет проверен на соответствие данному адресу Link Layer. При несовпадении адреса Link Layer и MAC-адреса пакет будет отброшен.

**Пример**

В данном примере показано, как настроить на коммутаторе действие отбрасывания для ND-сообщения, адрес Link Layer которого не соответствует MAC-адресу.

```
Switch# configure terminal
Switch(config)# ipv6 nd inspection policy policy1
Switch(config-nd-inspection)# validate source-mac
Switch(config-nd-inspection)#
```

**44-3 device-role**

Данная команда используется для указания роли подключенного устройства. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
device-role {host | router}
no device-role
```

**Параметры**

<b>host</b>	Укажите, чтобы настроить устройство в качестве узла (Host).
<b>router</b>	Укажите, чтобы настроить устройство в качестве маршрутизатора (Router).

**По умолчанию**

Роль устройства по умолчанию – Host.

**Режим ввода команды**

ND Inspection Policy Configuration Mode

**Использование команды**

Используйте данную команду, чтобы указать роль подключенного устройства. Так как по умолчанию устройство выполняет роль узла (Host), проверка сообщений NS и NA выполняется. Если устройство настроено в качестве маршрутизатора (Router), проверка сообщений NS и NA не выполняется. Сообщения NS и NA проверяются в соответствии с таблицей динамической привязки, информация о которой была получена из протокола ND или DHCP.

**Пример**

В данном примере показано, как создать политику ND под именем «policy1» и настроить устройство в качестве узла (Host).

```
Switch# configure terminal
Switch(config)# ipv6 nd inspection policy policy1
Switch(config-nd-inspection)# device-role host
Switch(config-nd-inspection)#
```

### 53-4 ipv6 nd inspection attach-policy

Данная команда используется для применения политики ND Inspection Policy на определенном интерфейсе. Используйте форму **no**, чтобы удалить политику ND Inspection Policy.

```
ipv6 nd inspection attach-policy [POLICY-NAME]
no ipv6 nd inspection attach-policy
```

#### Параметры

---

<i>POLICY-NAME</i>	(Опционально) Укажите имя политики ND Inspection Policy.
--------------------	--

---

#### По умолчанию

По умолчанию политика ND Inspection Policy не применена.

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

Данная команда используется для настройки физического порта и port-channel. Используйте данную команду, чтобы применить политику ND Inspection Policy на определенном интерфейсе. Если указано **no policy-name**, для политики по умолчанию действуют следующие правила:

- Сообщения NS/NA проверяются.
- MAC-адрес источника в заголовке пакета уровня 2 не проверяется.

#### Пример

В данном примере показано, как применить политику ND Inspection Policy под именем «policy1» на интерфейсе Ethernet 1/0/3.

```
Switch# configure terminal
Switch(config)# ipv6 nd inspection policy policy1
Switch(config-nd-inspection)# device-role host
Switch(config-nd-inspection)# validate source-mac
Switch(config-nd-inspection)# exit
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ipv6 nd inspection attach-policy policy1
Switch(config-if)#
```

## 44-5 show ipv6 nd inspection policy

Эта команда используется для отображения информации о политике защиты Router Advertisement (RA).

**show ipv6 nd inspection policy** [*POLICY-NAME*]

### Параметры

<i>POLICY-NAME</i>	(Необязательно) Укажите имя политики защиты IPv6 RA guard.
--------------------	--

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Если имя политики указано, отображаться будет информация только для указанной политики. Если имя политики не указано, отображаться будет информация для всех политик.

### Пример

В этом примере показано, как отобразить конфигурацию политики для политики с именем "inspect1".

```
Switch# show ipv6 nd inspection policy inspect1

Policy inspect1 configuration:
  Device Role: host
  Validate Source MAC: Enabled
  Target: eth1/0/1-1/0/2

Switch#
```

## 45. Команды Network Access Authentication

### 45-1 authentication guest-vlan

Эта команда используется для настройки параметров гостевой сети VLAN. Используйте форму **no** этой команды, чтобы удалить гостевую виртуальную локальную сеть.

```
authentication guest-vlan VLAN-ID
no authentication guest-vlan
```

#### Параметры

VLAN-ID	Укажите гостевую VLAN аутентификации.
---------	---------------------------------------

#### По умолчанию

Нет

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

Эта команда не может быть настроена, если указанная VLAN не существует как статическая VLAN. Хост не может получить доступ к сети, пока не пройдет аутентификацию. Если настроена гостевая VLAN, хосту разрешается доступ к гостевой VLAN без прохождения аутентификации. Во время аутентификации, если сервер RADIUS назначает пользователю VLAN, то пользователь будет авторизован в этой назначенной VLAN. Гостевая VLAN и назначение VLAN не действует на магистральном порту VLAN и туннельном порту VLAN. Обычно гостевая VLAN и назначение VLAN работают для хостов, которые подключаются к нетегированным портам. Это может вызвать неожиданное поведение, если оно работает на хостах, которые отправляют тегируемые пакеты.

Если режим хост-аутентификации установлен на **multi-host**, порт будет добавлен как порт-член гостевой VLAN, а PVID порта изменится на гостевую VLAN. Трафик, приходящий из гостевой VLAN, может быть передан независимо от того, прошла ли аутентификация. Трафик, приходящий из других VLAN, будет отбрасываться до тех пор, пока не пройдет аутентификацию. Когда один хост пройдет аутентификацию, порт покинет гостевую VLAN и будет добавлен в назначенную VLAN. PVID порта будет изменен на назначенную VLAN.

Если режим хоста аутентификации установлен на **multi-auth**, порт будет добавлен как порт-член гостевой VLAN, а PVID порта будет изменен на гостевую VLAN. Хостам, которым разрешен доступ к гостевой VLAN, запрещен доступ к другим VLAN до тех пор, пока они не пройдут аутентификацию. Когда один хост пройдет аутентификацию, порт останется в гостевой VLAN, PVID порта не будет изменен.

Если гостевая VLAN отключена, порт выйдет из гостевой VLAN и вернется в родную VLAN. PVID изменится на родную VLAN.

#### Пример

В этом примере показано, как указать VLAN 5 в качестве гостевой VLAN.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# authentication guest-vlan 5
Switch(config-if)#
```

## 45-2 authentication host-mode

Эта команда используется для указания режима аутентификации. Используйте форму по этой команды, чтобы вернуться к настройкам по умолчанию.

**authentication host-mode {multi-host | multi-auth}**  
**no authentication host-mode**

### Параметры

<b>multi-host</b>	Укажите порт для работы в режиме multi-host. Выполняется только одна аутентификация, и все хосты, подключенные к порту будут разрешены.
<b>multi-auth</b>	Укажите порт для работы в режиме multi-auth. Каждый узел будет проходить аутентификацию индивидуально.

### По умолчанию

По умолчанию используется **multi-auth**.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Если порт работает в режиме **multi-host** и аутентифицирован один из узлов, всем другим узлам будет разрешен доступ к порту. Согласно аутентификации 802.1X, если повторная аутентификация завершается неудачно или аутентифицированный пользователь выходит из учетной записи, порт будет заблокирован на период молчания (quiet period). Порт восстановит обработку пакетов EAPOL после периода молчания.

Если порт работает в режиме **multi-auth**, каждый узел должен проходить аутентификацию индивидуально для доступа к порту. Узел представлен своим MAC-адресом. Доступ есть только у авторизованных узлов.

### Пример

В данном примере показано, как назначить режим multi-host для порта Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication host-mode multi-host
Switch(config-if)#
```

## 45-3 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

#### Использование команды

Используйте эту команду для включения или отключения периодической повторной аутентификации для порта.

#### Пример

В этом примере показано, как включить периодическую повторную аутентификацию на порту 1.

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

## 45-4 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

<i>SECONDS</i>	Определяет таймер повторной аутентификации сеанса. Диапазон составляет от 1 до 65535.
----------------	--

#### По умолчанию

По умолчанию опция отключена.

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды



Используйте эту команду для настройки таймера повторной аутентификации.

### Пример

В этом примере показано, как настроить значение таймера повторной аутентификации на 200 для порта 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# authentication timer reauthentication 200
Switch(config-if)#
```

## 45-5 authentication timer restart

Данная команда используется для настройки таймера, по истечении которого станет возможна повторная аутентификация после последней неудачной попытки. При использовании формы **no** команда вернется к значениям по умолчанию.

**authentication timer restart** *SECONDS*  
**no authentication timer restart**

### Параметры

<i>SECONDS</i>	Указывает значение таймера перезапуска аутентификации. Диапазон составляет от 1 до 65535.
----------------	--

### По умолчанию

По умолчанию используется значение 60 секунд.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Коммутатор будет в режиме молчания (Quiet State) после неудачной попытки аутентификации до истечения времени таймера.

### Пример

В данном примере показано, как настроить значение таймера повторной аутентификации 20 для Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication timer restart 20
Switch(config-if)#
```

## 45-6 authentication username

Данная команда используется для создания пользователя в локальной базе данных аутентификации. При использовании формы **no** команда удалит пользователя из локальной базы данных аутентификации.

**authentication username** *NAME* **password** *PASSWORD* [**vlan** *VLAN-ID*]  
**no authentication username** *NAME* [**vlan**]

#### Параметры

<i>NAME</i>	Укажите имя пользователя, состоящее не более чем из 32 символов.
<b>password</b> <i>PASSWORD</i>	Укажите, чтобы задать пароль для MAC-аутентификации. Если указан пароль в обычном текстовом виде, длина строки не может превышать 32 символа.
<b>vlan</b> <i>VLAN-ID</i>	Указывает назначаемую сеть VLAN.

#### По умолчанию

Нет

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Данная команда используется для настройки локальной базы данных для аутентификации пользователей.

#### Пример

В данном примере показано, как создать локальную учетную запись с именем пользователя user1 и паролем pass1.

```
Switch# configure terminal
Switch(config)# authentication username user1 password pass1
Switch(config)#
```

## 45-7 clear authentication sessions

Данная команда используется для удаления сессий аутентификации.

**clear authentication sessions** { **dot1x** | **all** | **interface** *INTERFACE-ID* [**mac** | **wac** [**dot1x**] | **mac-address** *MAC ADDRESS*]

#### Параметры

<b>dot1x</b>	Укажите для удаления всех сессий dot1x.
<b>all</b>	Укажите для удаления всех сессий.
<b>interface</b> <i>INTERFACE-ID</i>	Укажите для удаления сессий порта.
<b>mac-address</b> <i>MAC ADDRESS</i>	Укажите для удаления всех сессий определенного пользователя.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Команда используется для удаления сессий аутентификации.

#### Пример

В данном примере показано, как удалить сессии аутентификации на Ethernet 1/0/1.

```
Switch# clear authentication sessions interface ethernet 1/0/1
Switch#
```

## 45-8 authentication max users

Данная команда используется для настройки максимального количества аутентифицированных пользователей для всей системы или для порта. При использовании формы **no** команда вернется к значениям по умолчанию.

**authentication max users** *NUMBER*  
**no authentication max users**

#### Параметры

<i>NUMBER</i>	Указывает для установки максимального числа аутентифицированных пользователей. Диапазон составляет от 1 до 1000.
---------------	--

#### По умолчанию

По умолчанию ограничений нет.

#### Режим ввода команды

Global Configuration Mode  
 Interface Configuration Mode

#### Использование команды

Команда может использоваться в режиме Global Configuration Mode и Interface Configuration Mode.

Если команда настроена в режиме Global Configuration Mode, задается ограничение максимального количества пользователей на всю систему.

Если команда настроена в режиме Interface Configuration Mode, задается ограничение максимального количества пользователей на интерфейс.

Максимальное число пользователей включает пользователей 802.1X, MAC-based Access Control и WAC.

Также команда имеет следующее ограничение:

- Если новое число максимального количества пользователей меньше, чем текущее количество пользователей, команда будет отклонена, и появится сообщение об ошибке.

### Пример

В этом примере показано, как установить максимальное количество аутентифицированных пользователей для системы.

```
Switch# configure terminal
Switch(config)# authentication max users 256
Switch(config)#
```

## 45-9 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

### Использование команды

Используйте эту команду для включения или отключения приема авторизованной конфигурации. Когда авторизация включена для аутентификации, авторизованные атрибуты (например, VLAN), назначенные сервером RADIUS, будут приняты, если статус авторизации включен.

### Пример

В этом примере показано, как включить статус авторизации.

```
Switch# configure terminal
Switch(config)# no authorization disable
Switch(config)#
```

## 45-10 show authentication sessions

Данная команда используется для просмотра информации об аутентификации.

**show authentication sessions [dot1x | interface *INTERFACE-ID* [, | -] [mac | wac [dot1x] | mac-address *MAC-ADDRESS*]**

#### Параметры

<b>dot1x</b>	(Опционально) Укажите для отображения всех сессий dot1x.
<b>interface <i>INTERFACE-ID</i></b>	(Опционально) Укажите порт для отображения.
<b>,</b>	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
<b>-</b>	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
<b>mac-address <i>MAC-ADDRESS</i></b>	(Опционально) Укажите для отображения определенного пользователя.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте команду без параметров, чтобы включить отображение сессий со всех портов.

#### Пример

В этом примере показано, как отобразить сессии на порту 1.

```
Switch#show authentication sessions interface eth1/0/1
```

```
Interface: eth1/0/1
MAC Address: 00-E0-4C-68-2D-6F
Authentication VLAN: 1
Authentication State: Success
Authentication Username: abc
Aging Time: 3144 sec
Method   State
 802.1X  : Success, Selected
802.1X Authenticator State: AUTHENTICATED
802.1X Backend State: IDLE

Total Authenticating Hosts: 0
Total Authenticated Hosts: 1
Total Blocked Hosts: 0

Switch#
```

#### Отображаемые параметры

<b>Interface</b>	Полученный интерфейс узла аутентификации.
<b>MAC Address</b>	MAC-адрес узла аутентификации.
<b>Authentication VLAN</b>	Исходная VLAN хоста, в которой начинается аутентификация.
<b>Authentication State</b>	Статус аутентификации хоста. <ul style="list-style-type: none"> <li>• Start - Хост получен, но аутентификация не начата.</li> <li>• Initialization - ресурс аутентификации готов, но новая аутентификация не начата.</li> <li>• Authenticating - Хост проходит аутентификацию.</li> <li>• Failure - Сбой аутентификации.</li> <li>• Success - хост прошел аутентификацию.</li> </ul>
<b>Authentication Username</b>	Указывает имя пользователя узла.
<b>Assigned VLAN</b>	Эффективно назначенный идентификатор VLAN, который был авторизован после прохождения хостом аутентификации.
<b>Method</b>	Метод аутентификации, например 802.1X.
<b>State</b>	Состояние аутентификации метода. <ul style="list-style-type: none"> <li>• Authenticating - Хост проходит аутентификацию этим методом.</li> <li>• Success - Хост прошел аутентификацию этим методом.</li> <li>• Selected - Результат аутентификации этим методом принимается и анализируется системой для хоста.</li> </ul>

	<ul style="list-style-type: none"> <li>• Failure - хост не прошел аутентификацию этим методом.</li> <li>• No Information - Информация об аутентификации недоступна.</li> </ul>
<b>Aging Time/Block Time</b>	<p><b>Aging Time</b> (Время старения) - определяет период времени, в течение которого аутентифицированный узел будет находиться в аутентифицированном состоянии. По истечении времени старения хост будет переведен обратно в состояние без аутентификации.</p> <p><b>Blocked Time</b> - Если хост не прошел аутентификацию, следующая аутентификация не начнется в течение времени блокировки, пока пользователь не очистит состояние входа вручную.</p>
<b>802.1X Authenticator State</b>	<p>Указывает состояние PAE аутентификатора 802.1X: Может иметь одно из следующих значений:</p> <p><b>INITIALIZE</b> - Указывает, что аутентификатор инициализирует машину состояния и готов к аутентификации клиента.</p> <p><b>DISCONNECTED</b> - Указывает, что инициализация машины состояний завершена, но к этому порту не подключен ни один клиент.</p> <p><b>CONNECTING</b> - Указывает, что коммутатор обнаружил подключающегося к этому порту клиента. PAE попытается установить связь с агентом.</p> <p><b>AUTHENTICATING</b> - Указывает, что суппликант проходит аутентификацию.</p> <p><b>AUTHENTICATED</b> - Указывает на то, что аутентификатор успешно аутентификацию клиента.</p> <p><b>ABORTING</b> - Указывает, что процедура аутентификации преждевременно прерывается из-за получения запроса повторной аутентификации, кадра EAPOL-Start, кадра EAPOL-Logoff или тайм-аута аутентификации.</p> <p><b>HELD</b> - Указывает, что машина состояния игнорирует и отбрасывает все пакеты EAPOL, чтобы предотвратить атаки грубой силы. Это состояние переходит из состояния AUTHENTICATING после сбоя аутентификации.</p> <p><b>FORCE_AUTH</b> - Указывает, что клиент всегда авторизован.</p> <p><b>FORCE_UNAUTH</b> - Указывает, что клиент всегда неавторизован.</p>
<b>802.1X Backend State</b>	<p>Указывает состояние бэкенда 802.1X PAE. Это может быть одно из следующих значений:</p> <p><b>REQUEST</b> - Указывает, что машина состояния получила пакет запроса EAP от сервера аутентификации и передает этот пакет суппликанту в виде инкапсулированного кадра EAPOL.</p> <p><b>RESPONSE</b> - Указывает, что машина состояния получила инкапсулированный EAPOL пакет EAP Response от агента и передает этот пакет EAP серверу аутентификации.</p> <p><b>SUCCESS</b> - Указывает, что сервер аутентификации</p>

подтвердил, что клиент является законным клиентом. Машина состояния backend уведомит машину состояния PAE аутентификатора и суппликанта.

**FAIL** - Указывает, что сервер аутентификации подтвердил, что supplicant является нелегальным клиентом. Машина состояния backend уведомит машину состояния PAE аутентификатора и клиента.

**TIMEOUT** - Указывает на то, что сервер аутентификации или супбликант вышел по тайм-ауту.

**IDLE** - В этом состоянии машина состояния ожидает сигнала машины состояния аутентификатора о начале нового сеанса аутентификации.

**INITIALIZE** - Указывает, что аутентификатор инициализирует машину состояния.

---



## 46. Команды Network Protocol Port Protection

### 46-1 network-protocol-port protect

Эта команда используется для включения функции защиты порта сетевого протокола. Используйте форму **no** этой команды для отключения этой функции.

```
network-protocol-port protect {tcp | udp}
no network-protocol-port protect {tcp | udp}
```

#### Параметры

<b>tcp</b>	Указывает на защиту порта TCP.
<b>udp</b>	Указывает для защиты порт UDP.

#### По умолчанию

По умолчанию эта функция включена.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте эту команду для включения или отключения функции защиты порта сетевого протокола. Если порт защищен, коммутатор не будет отправлять ответные пакеты на закрытый порт TCP или UDP.

#### Пример

В этом примере показано, как включить защиту портов TCP.

```
Switch#configure terminal
Switch(config)#network-protocol-port protect tcp
Switch(config)#
```

### 46-2 show network-protocol-port protect

Эта команда используется для отображения информации о защите порта сетевого протокола.

```
show network-protocol-port protect
```

#### Параметры

Нет

#### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте эту команду для отображения информации о защите порта сетевого протокола.

### Пример

В данном примере показано, как отобразить информацию о защите порта сетевого протокола.

```
Switch#show network-protocol-port protect

TCP Port protect state: Enabled
UDP Port protect state: Enabled

Switch#
```

## 47. Команды Port Security

### 47-1 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

<b>all</b>	Укажите, чтобы удалить все динамически изученные безопасные MAC- адреса.
<b>address MAC-ADDR</b>	Укажите, чтобы удалить указанные динамически изученные безопасные записи на основе введенного MAC-адреса.
<b>interface INTERFACE-ID</b>	Укажите, чтобы удалить все динамически изученные безопасные записи на указанном интерфейсе.
<b>,</b>	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
<b>-</b>	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
<b>vlan VLAN-ID</b>	Укажите, чтобы удалить динамически изученные записи, информация о которых была получена через указанную VLAN.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### 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#
```

### 47-2 show port-security

Данная команда используется для просмотра текущих настроек Port Security.

```
show port-security [[interface INTERFACE-ID [, | -]] [address]]
```

**Параметры**

<b>interface</b> <i>INTERFACE-ID</i>	(Опционально) Укажите ID интерфейса, который необходимо отобразить.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
<b>address</b>	(Опционально) Укажите для отображения безопасных MAC-адресов, включая настроенные и изученные адреса.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Команда используется для отображения текущих настроек Port Security.

**Пример**

В данном примере показано, как включить отображение настроек Port Security для Ethernet с 1/0/1 по 1/0/3.

```
Switch#show port-security interface ethernet 1/0/1-3

D:Delete-on-Timeout  P:Permanent
Interface      Max  Curr  Violation  Violation  Security  Admin  Current
No.            No.  No.   Act.       Count      Mode    State  State
-----
eth1/0/1      5    2    Restrict  0           D  Enabled Forwarding
eth1/0/2     10   10   Shutdown  0           D  Enabled  Err-disabled
eth1/0/3     10    0   Shutdown  0           P  Disabled -

Switch#
```

**47-3 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 от отправку SNMP-уведомлений.

```
snmp-server enable traps port-security [trap-rate TRAP-RATE]
no snmp-server enable traps port-security [trap-rate]
```

**Параметры**

<b>trap-rate</b> <i>TRAP-RATE</i>	(Опционально) Укажите количество трапов в секунду. Доступен диапазон значений от 0 до 1000. Значение по умолчанию 0 означает, что SNMP trap будет генерироваться для каждого нарушения безопасности.
-----------------------------------	--

**По умолчанию**

По умолчанию функция отключена.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Команда используется для включения или отключения отправки SNMP-уведомлений при обнаружении функционалом Port Security недопустимых адресов.

**Пример**

В данном примере показано, как включить отработку трапов при обнаружении функционалом Port Security недопустимых адресов и установить количество трапов в секунду, равное 3.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps port-security trap-rate 3
Switch(config)#
```

**47-4 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**

<b>maximum</b> <i>VALUE</i>	(Опционально) Укажите максимальное число разрешенных безопасных MAC-адресов. Если не указано, значение по умолчанию – 32. Доступен диапазон значений от 0 до 6656.
<b>protect</b>	(Опционально) Укажите, если необходимо отбрасывать все пакеты с незащищенных узлов на уровне port-security без возрастания счетчика нарушения безопасности (security-violation).
<b>restrict</b>	(Опционально) Укажите, если необходимо отбрасывать все пакеты с незащищенных узлов на уровне port-security, с возрастанием счетчика нарушения безопасности (security-violation) и записью в системный журнал (system log).
<b>shutdown</b>	(Опционально) Укажите для отключения порта, если

	произошло нарушение безопасности и для записи в системный журнал (system log).
<b>permanent</b>	(Опционально) В данном режиме все изученные MAC-адреса не будут удалены, пока пользователь не удалит их вручную.
<b>delete-on timeout</b>	(Опционально) В данном режиме все изученные MAC-адреса будут удалены, когда запись устареет, или если пользователь удалит записи вручную.
<b>mac-address MAC-ADDRESS</b>	(Опционально) Укажите, чтобы добавить безопасный MAC-адрес для получения доступа к порту.
<b>permanent</b>	(Опционально) Укажите, чтобы задать безопасный постоянно настроенный MAC-адрес порта. Данная запись является такой же, как изученная в режиме Permanent Mode.
<b>vlan VLAN-ID</b>	(Опционально) Укажите VLAN. Если VLAN не указана, MAC-адрес будет изучен в соответствии с PVID.

### По умолчанию

По умолчанию опция отключена.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Когда включена функция Port Security, если режим порта port mode настроен как **delete-on-timeout**, порт автоматически будет изучать безопасные записи и хранить их, пока не истечет их время тайм-аута. Время хранения этих записей зависит от настроек, заданных командой **switchport port-security aging**. Если режим порта задан как постоянный (permanent), он будет автоматически изучать безопасные записи с неистекающим тайм-аутом. Автоматически изученные безопасные записи будут храниться в текущем файле конфигурации (running configuration).

При изменении состояния безопасности режима порта (port mode-security) счетчик нарушений будет сброшен, записи Auto-permanent будут преобразованы в соответствующие динамические записи. При отключении режима порта port-security автоматически изученные безопасные записи будут удалены, включая динамические и постоянные (Permanent), а также счетчик нарушений. При изменении настройки VLAN автоматически изученные динамические безопасные записи будут удалены.

Постоянные безопасные записи будут храниться в текущем файле конфигурации (running configuration) и могут быть сохранены в NVRAM при использовании команды **copy**. Настроенные пользователем безопасные MAC-адреса будут подсчитываться в максимальном количестве MAC-адресов на порт.

Так как постоянная (permanent) безопасная запись Port Security включена на порту, MAC-адрес нельзя перенести на другой порт.

При изменении настроек изученные адреса останутся неизменными, если максимальное число будет увеличено. Если максимальное число будет изменено на меньшее, чем существующее число изучаемых записей, команда будет отклонена.

Порт с поддержкой Port Security имеет следующие ограничения:

- Функция Port Security не может функционировать одновременно с 802.1X, MAC-based Access Control (управление доступом на основе MAC), WAC и IMPV, 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)#
```

## 47-5 switchport port-security aging

Данная команда позволяет задать время старения (aging time) для динамически изученных безопасных адресов на интерфейсе. При использовании формы **no** команда вернется к значениям по умолчанию.

```
switchport port-security aging {time MINUTES | type {absolute | inactivity}}
no switchport port-security aging {time | type}
```

### Параметры

<b>time</b> <i>MINUTES</i>	Укажите время старения (aging time) для динамически изученных безопасных адресов на порту в минутах. Доступен диапазон значений от 0 до 1440.
<b>type</b>	Укажите тип старения.
<b>absolute</b>	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.
<b>inactivity</b>	Укажите, чтобы задать тип inactivity. Все безопасные адреса на данном порту устаревают, только если нет трафика с безопасного адреса источника в течение указанного времени.

**По умолчанию**

По умолчанию функция отключена.  
 Время хранения по умолчанию – 0 минут.  
 Тип хранения по умолчанию – **absolute**.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Команда используется для отключения процесса старения записей, а также для того, чтобы задать время старения динамически изученных безопасных записей. Для того чтобы задать тип **inactivity**, должна быть включена функция FDB Table Ageing.

**Пример**

В этом примере показано, как применить время старения для автоматически выученных безопасных MAC-адресов на порту 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport port-security aging time 1
Switch(config-if)#
```

**47-6 port-security limit**

Данная команда позволяет задать максимальное количество безопасных MAC-адресов в системе или на указанной VLAN. При использовании формы **no** команда вернется к настройкам по умолчанию.

**port-security limit** *VALUE*  
**no port-security limit**

**Параметры**

<i>VALUE</i>	Укажите максимальное число записей Port Security, которое
--------------	---



может быть изучено в системе или в указанной VLAN.  
Доступен диапазон значений от 1 до 3328. 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

#### **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)#
```

---

## 48. Команды Power over Ethernet (PoE) Commands (только для ТГК-125-24/4д-2П и ТГК-125-48/4д-2П)

### 48-1 poe pd description

Эта команда используется для настройки описания для PD, подключенного к порту PoE. Используйте **no** для очистки описания.

```
poe pd description TEXT
no poe pd description
```

#### Параметры

<i>TEXT</i>	Указывает строку, описывающую PD, подключенный к интерфейсу PoE. Максимальная длина - 32 символа.
-------------	---

#### По умолчанию

Нет

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

Эта команда используется для настройки описания PD, подключенного к порту.

#### Пример

В этом примере показано, как настроить описание PoE PD на порту 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe pd description For VoIP usage
Switch(config-if)#
```

### 48-2 poe pd legacy-support

Эта команда используется для включения поддержки устаревшего PD. Используйте форму **no** этой команды, чтобы отключить ее.

```
poe pd legacy-support
no poe pd legacy-support
```

#### Параметры

Нет

**По умолчанию**

По умолчанию эта опция отключена.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Используйте эту команду, чтобы включить поддержку устаревших PD, подключенных к порту. Если поддержка устаревших устройств отключена, система не будет подавать питание на устаревшие PD.

**Пример**

В этом примере показано, как включить поддержку устаревших технологий для PD, подключенных к порту 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe pd legacy-support
Switch(config-if)#
```

**48-3 poe pd priority**

Эта команда используется для настройки приоритета для подачи питания на порт. Используйте форму **po** этой команды для возврата к настройкам по умолчанию.

```
poe pd priority {critical | high | low}
no poe pd priority
```

**Параметры**

<b>critical</b>	Укажите, что PD, подключенный к порту, имеет наивысший приоритет.
<b>high</b>	Укажите, что PD, подключенный к порту, получает второй высокий приоритет.
<b>low</b>	Укажите, что PD, подключенный к порту, имеет самый низкий приоритет.

**По умолчанию**

По умолчанию этот параметр установлен как **низкий**.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Поскольку бюджет мощности ограничен, при добавлении в систему большего количества PD источник питания может оказаться недостаточным для обеспечения питания. Система PoE переходит в критическую секцию питания, когда оставшегося источника питания недостаточно для обслуживания нового

добавленного PD. Будет ли подаваться питание на новый добавленный PD, зависит от политики, настроенной командой **poe policy preempt**.

Если параметр вытеснения политики отключен, политика будет обслуживаться в первую очередь. Таким образом, новый PD не будет обслуживаться, если источник питания на исходе. Если параметр вытеснения политики включен, питание, предоставляемое PD с более низким приоритетом, может быть вытеснено, чтобы освободить питание для нового подключенного PD с более высоким приоритетом.

### Пример

В этом примере показано, как настроить приоритет порта 1 на первый приоритет.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe pd priority critical
Switch(config-if)#
```

## 48-4 poe policy preempt

Эта команда используется для разрешения отключения PD, имеющего более низкий приоритет, чтобы в условиях нехватки питания передать питание новому подключенному PD с более высоким приоритетом. Для возврата к настройкам по умолчанию используйте форму **no** этой команды.

**poe unit policy preempt**  
**no poe unit policy preempt**

### Параметры

Нет

### По умолчанию

По умолчанию эта опция отключена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Поскольку бюджет питания ограничен, по мере добавления в систему большего количества PD, источник питания может оказаться недостаточным для обеспечения питания. Система PoE переходит в критическую секцию питания, когда оставшегося бюджета питания недостаточно для обслуживания нового добавленного PD.

Команда **poe policy preempt** настраивает, следует ли отключать PD с более низким приоритетом, чтобы передать питание новому подключенному PD с более высоким приоритетом в условиях нехватки питания. Если параметр вытеснения политики отключен, политика будет обслуживаться в первую очередь. Таким образом, новый PD не будет обслуживаться, если бюджет питания исчерпан.

Если параметр вытеснения политики включен, мощность, предоставленная PD с более низким приоритетом, может быть вытеснена, чтобы освободить мощность для нового подключенного PD с более высоким приоритетом.

## Пример

В этом примере показано, как настроить вытесняющий режим политики обслуживания питания системы PoE.

```
Switch# configure terminal
Switch(config)# poe unit 1 policy preempt
Switch(config)#
```

## 48-5 poe power-inline

Эта команда используется для настройки режима управления питанием для портов PoE. Используйте форму **no** этой команды для удаления ассоциации профилей временного диапазона или возврата режима к настройкам по умолчанию.

**poe power-inline {auto [max MAX-WATTAGE] [time-range PROFILE-NAME] | never}**  
**no poe power-inline [auto {max | time-range}]**

### Параметры

<b>auto</b>	Указывает, чтобы включить автоматическое обнаружение PD и обеспечить питание PD.
<b>max MAX-WATTAGE</b>	(Опционально) Указывается для установки максимальной мощности, которая может быть предоставлена автоопределяемому PD. Если этот параметр не указан, то класс PD автоматически определяет максимальную мощность, которая может быть предоставлена. Диапазон допустимых значений максимальной мощности составляет от 1000 мВт до 30000 мВт.
<b>time-range PROFILE-NAME</b>	(Опционально) Указывает имя профиля временного диапазона для разграничения периода активации.
<b>never</b>	Указывает на отключение подачи питания на PD, подключенный к порту.

### По умолчанию

По умолчанию этот параметр установлен как **auto**.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Если порт установлен в auto mode, порт самостоятельно обнаружит PD и обеспечит его питанием. Пользователь может явно указать максимальное значение мощности, которое может быть предоставлено порту. Если максимальное значение мощности не указано, то класс БП автоматически определяет максимальную мощность, которая может быть предоставлена. БП не будет предоставлен, если он запросит мощность, превышающую максимальную.

Используйте эту команду, чтобы также указать временной диапазон для порта. Если порт PoE связан с профилем временного диапазона, он будет активирован только в течение временного интервала,

указанного в профиле. То есть, питание на PD не будет подаваться в течение времени, выходящего за рамки указанного временного диапазона.

При выполнении команды **no poe power-inline** режим управления питанием будет возвращен к настройкам по умолчанию.

Для настройки команды указанный профиль временного диапазона не обязательно должен существовать. Если профиль временного диапазона не существует, команда действует так, как будто временной диапазон не указан.

### Пример

В этом примере показано, как включить обнаружение PD и автоматически подавать питание на устройство PoE, подключенное к порту 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe power-inline auto
Switch(config-if)#
```

В этом примере показано, как настроить порт PoE 1 на разрешение питания устройств мощностью менее 7000 мВт.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe power-inline auto max 7000
Switch(config-if)#
```

В этом примере показано, как отключить обнаружение PD и не подавать питание на устройство PoE, подключенное к порту 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe power-inline never
Switch(config-if)#
```

В этом примере показано, как объединить профиль временного диапазона под названием "day-time" с портом PoE 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe power-inline auto time-range day-time
Switch(config-if)#
```

## 48-6 poe usage-threshold

Эта команда используется для настройки порога использования для записи журнала. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

**poe unit usage-threshold PERCENTAGE**  
**no poe unit usage-threshold**

#### Параметры

<i>PERCENTAGE</i>	Указывает порог использования для создания журнала. Диапазон значений от 1 до 99. Единица измерения - процент.
-------------------	--

#### По умолчанию

По умолчанию это значение равно 99.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Когда настроен порог использования, если использование PSE превысит настроенный порог, будет записан журнал EXCEED. Как только процент уменьшится и станет ниже порогового значения, будет записан журнал RECOVER.

#### Пример

В данном примере показано, как настроить порог использования на 50%.

```
Switch# configure terminal
Switch(config)# poe unit 1 usage-threshold 50
Switch(config)#
```

## 48-7 snmp-server enable traps poe

Эта команда используется для включения отправки уведомлений PoE. Используйте форму **no** этой команды чтобы отключить отставку уведомлений о питании по Ethernet.

**snmp-server enable traps poe**  
**no snmp-server enable traps poe**

#### Параметры

Нет

#### По умолчанию

По умолчанию эта опция отключена.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте эту команду для включения или отключения отправки уведомлений PoE.

## Пример

В этом примере показано, как включить отправку уведомлений PoE.

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

## 48-8 clear poe statistic

Эта команда используется для очистки счетчиков статистики на порту.

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

### Параметры

<b>all</b>	Указывает очистку статистики PoE для всех интерфейсов.
<b>interface <i>INTERFACE-ID</i></b>	Указывает идентификатор интерфейса.
<b>,</b>	(Опционально) Указывает серию интерфейсов или отделяет диапазон интерфейсов от предыдущего диапазона. Пробелы до и после запятой не нужны.
<b>-</b>	(Опционально) Указывает диапазон интерфейсов. Без пробелов до и после дефиса.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Для записи статистики на портах имеются счетчики, которые можно показать, введя команду **show poe power-inline statistics command**. Используйте эту команду для очистки всех значений счетчиков на порту.

## Пример

В данном примере показано, как очистить статистику на интерфейсе eth1/0/1.

```
Switch# clear poe statistic interface eth1/0/1
Switch#
```

## 48-9 show poe power-inline

Эта команда используется для отображения статуса PoE для указанного порта PoE или для всех портов PoE на коммутаторе.

**show poe power-inline [*INTERFACE-ID* [, | -]] {status | configuration | statistics | measurement | lldp-classification}**



**Параметры**

<i>INTERFACE-ID</i>	(Опционально) Укажите интерфейс, который будет отображаться.
,	(Опционально) Указывает серию интерфейсов или отделяет диапазон интерфейсов от предыдущего диапазона. Пробелы до и после запятой не нужны.
-	(Опционально) Указывает диапазон интерфейсов. Без пробелов до и после дефиса.
<b>status</b>	Указывает для отображения состояния порта PoE.
<b>configuration</b>	Указывает на отображение информации о конфигурации порта.
<b>statistics</b>	Указывает на отображение счетчиков ошибок порта.
<b>measurement</b>	Указывает для отображения напряжения, тока, потребляемой мощности и температуры порта.
<b>lldp-classification</b>	Указывает на отображение классификации уровня канала данных с использованием информации о мощности через MDI TLV.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Эта команда используется для отображения статуса PoE портов, состояния конфигурации линии электропитания, счетчиков статистики, результатов измерений и информации о классификации уровня канала передачи данных. Если ID интерфейса не указан в этой команде, то будут отображены все интерфейсы PoE. Отображаются только интерфейсы с поддержкой PoE.

**Пример**

В этом примере показано, как отобразить состояние питания PoE в линии.

```
Switch#show poe power-inline status

Interface      State      Class    Max(W)  Used(W)  Description
-----
eth1/0/1      delivering class-1  7.0     3.4     For VoIP usage
eth1/0/2      searching  n/a     0.0     0.0
eth1/0/3      searching  n/a     0.0     0.0
eth1/0/4      searching  n/a     0.0     0.0
eth1/0/5      searching  n/a     0.0     0.0
eth1/0/6      searching  n/a     0.0     0.0
eth1/0/7      searching  n/a     0.0     0.0
eth1/0/8      searching  n/a     0.0     0.0
eth1/0/9      searching  n/a     0.0     0.0
eth1/0/10     searching  n/a     0.0     0.0
eth1/0/11     searching  n/a     0.0     0.0
eth1/0/12     searching  n/a     0.0     0.0
eth1/0/13     searching  n/a     0.0     0.0
eth1/0/14     searching  n/a     0.0     0.0
eth1/0/15     searching  n/a     0.0     0.0
eth1/0/16     searching  n/a     0.0     0.0
eth1/0/17     searching  n/a     0.0     0.0
eth1/0/18     searching  n/a     0.0     0.0
eth1/0/19     searching  n/a     0.0     0.0
eth1/0/20     searching  n/a     0.0     0.0
eth1/0/21     searching  n/a     0.0     0.0
eth1/0/22     searching  n/a     0.0     0.0
eth1/0/23     searching  n/a     0.0     0.0
eth1/0/24     searching  n/a     0.0     0.0

Faulty code
[1] MPS (Maintain Power Signature) Absent
[2] PD short
[3] Overload
[4] Power Denied
[5] Thermal Shutdown
[6] Startup Failure
[7] Classification Failure

Switch#
```

**Отображаемые параметры**

<b>Interface</b>	Идентификатор интерфейса PoE.
<b>State</b>	Состояние порта может быть одним из следующих:

---

**Disabled:** Функция PSE отключена.

**Searching:** Удаленный PD не подключен.

**Requesting** (запрос): Удаленный БП подключен, но PSE еще не подает питание.

**Delivering:** Удаленный БП получает питание от системы PoE.

**Faulty[X]:** Обнаружение устройства или питаемое устройство находится в неисправном состоянии. X -это номер кода ошибки.

[1] - MPS (Maintain Power Signature) Отсутствует.

[2] - Короткое замыкание БП.

[3] - Перегрузка.

[4] - Отказ в питании.

[5] - Тепловое отключение.

[6] - Сбой запуска.

[7] - Сбой классификации (IEEE 802.3at).

---

<b>Class</b>	Классификация IEEE: N/A или значение из класса IEEE от 0 до 4.
<b>Max(W)</b>	Максимальное количество мощности, которое может быть выделено питаемому устройству в ваттах.
<b>Used(W)</b>	Количество энергии, выделяемой в настоящее время портам PoE, в ваттах.
<b>Description</b>	Сконфигурированное описание подключенного PD.

---

В этом примере показано, как отобразить конфигурацию PoE power inline.

```
Switch#show poe power-inline configuration

Interface Admin Priority Legacy-Support Time-Range
-----
eth1/0/1 auto(M) critical enabled
eth1/0/2 auto low disabled
eth1/0/3 auto low disabled
eth1/0/4 auto low disabled
eth1/0/5 auto low disabled
eth1/0/6 auto low disabled
eth1/0/7 auto low disabled
eth1/0/8 auto low disabled
eth1/0/9 auto low disabled
eth1/0/10 auto low disabled
eth1/0/11 auto low disabled
eth1/0/12 auto low disabled
eth1/0/13 auto low disabled
eth1/0/14 auto low disabled
eth1/0/15 auto low disabled
eth1/0/16 auto low disabled
eth1/0/17 auto low disabled
eth1/0/18 auto low disabled
eth1/0/19 auto low disabled
eth1/0/20 auto low disabled
eth1/0/21 auto low disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

### Отображаемые параметры

<b>Interface</b>	Идентификатор интерфейса PoE.
<b>Admin</b>	<p>Настраиваемый пользователем режим может быть одним из следующих:</p> <p><b>Auto</b> (Авто): устройство с питанием будет автоматически обнаружено, а максимальная мощность будет основана на результатах обнаружения.</p> <p><b>Auto(M)</b>: Питаемое устройство будет автоматически обнаружено, а максимальная мощность будет равна значению, настроенному пользователем.</p> <p><b>Never (Никогда)</b>: Питаемое устройство не будет обнаружено, и питание на порт не подается.</p>
<b>Priority</b>	Приоритет, используемый для определения очередности обслуживания при ограничении мощности в пределах энергоблока.
<b>Legacy-Support</b>	<p><b>Enabled</b> (Включено): Устаревший БП может быть обнаружен.</p> <p><b>Disabled</b>: Устаревший БП не может быть обнаружен.</p>

---

**Time-Range**                      Имя профиля временного диапазона, который устанавливает временные рамки активации для порта.

---

В этом примере показано, как отобразить статистику PoE power inline.

```
Switch#show poe power-inline statistics

Interface  MPS Absent  Overload  Short  Power Denied  Invalid Signature
-----
eth1/0/1   2          5         0       10       7
eth1/0/2   0          0         0       0        9
eth1/0/3   0          0         0       0        9
eth1/0/4   0          0         0       0       10
eth1/0/5   0          0         0       0      157
eth1/0/6   0          0         0       0      157
eth1/0/7   0          0         0       0      156
eth1/0/8   0          0         0       0      158
eth1/0/9   0          0         0       0      166
eth1/0/10  0          0         0       0      165
eth1/0/11  0          0         0       0      165
eth1/0/12  0          0         0       0      166
eth1/0/13  0          0         0       0      143
eth1/0/14  0          0         0       0      143
eth1/0/15  0          0         0       0      143
eth1/0/16  0          0         0       0      144
eth1/0/17  0          0         0       0      166
eth1/0/18  0          0         0       0      166
eth1/0/19  0          0         0       0      166
eth1/0/20  0          0         0       0      161
eth1/0/21  0          0         0       0      163

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

### Отображаемые параметры

<b>MPS Absent</b>	Увеличивается, если PSE перестает подавать питание на PI из-за того, что PSE не может контролировать действующие MPS PD на PI.
<b>Overload</b>	Если PD потребляет слишком много энергии, превышая максимальную выходную мощность, которую может обеспечить порт, счетчик перегрузки увеличивается.
<b>Short</b>	Если внутренняя цепь PD по какой-то причине закорочена, этот счетчик увеличивается.
<b>Power Denied</b>	Если программная система PoE решает запретить подачу питания на подключенный PD, этот счетчик увеличивается.
<b>Invalid Signature</b>	Увеличивается, если PSE обнаруживает PD, у которого недействительная подпись PD.

В этом примере показано, как отобразить измерение мощности PoE в линии.

```
Switch#show poe power-inline measurement
```

Interface	Voltage (V)	Current (mA)	Temperature (C)	Power (W)
eth1/0/1	54.2	109	35	5.9
eth1/0/2	n/a	n/a	n/a	n/a
eth1/0/3	n/a	n/a	n/a	n/a
eth1/0/4	n/a	n/a	n/a	n/a
eth1/0/5	n/a	n/a	n/a	n/a
eth1/0/6	n/a	n/a	n/a	n/a
eth1/0/7	n/a	n/a	n/a	n/a
eth1/0/8	n/a	n/a	n/a	n/a
eth1/0/9	n/a	n/a	n/a	n/a
eth1/0/10	n/a	n/a	n/a	n/a
eth1/0/11	n/a	n/a	n/a	n/a
eth1/0/12	n/a	n/a	n/a	n/a
eth1/0/13	n/a	n/a	n/a	n/a
eth1/0/14	n/a	n/a	n/a	n/a
eth1/0/15	n/a	n/a	n/a	n/a
eth1/0/16	n/a	n/a	n/a	n/a
eth1/0/17	n/a	n/a	n/a	n/a
eth1/0/18	n/a	n/a	n/a	n/a
eth1/0/19	n/a	n/a	n/a	n/a
eth1/0/20	n/a	n/a	n/a	n/a
eth1/0/21	n/a	n/a	n/a	n/a

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

В этом примере показано, как отобразить классификацию PoE power inline LLDP.

```
Switch# show poe power-inline lldp-classification
```

```
Interface eth1/0/1
```

```
PSE TX information:
```

```
Power type; type 2 PSE
```

```
Power source: primary power source
```

```
Power priority: low
```

```
PD requested power value: 25.0W
```

```
PSE allocated power value: 25.0W
```

```
Information from PD:
```

```
Power type: type 2 PD
```

```
Power source: PSE
```

```
Power priority: unknown
```

```
PD requested power value: 25.0W
```

```
PSE allocated power value: 25.0W
```

```
Interface eth1/0/2
```

```
PSE TX information:
```

```
Power type; type 2 PSE
```

```
Power source: primary power source
```

```
Power priority: high
```

```
PD requested power value: 0.0W
```

```
PSE allocated power value: 0.0W
```

```
Information from PD:
```

```
none
```

```
Interface eth1/0/3
```

```
PSE TX information:
```

```
Power type; type 2 PSE
```

```
Power source: primary power source
```

```
Power priority: low
```

```
PD requested power value: 20.0W
```

```
PSE allocated power value: 20.0W
```

```
Information from PD:
```

```
Power type: type 2 PD
```

```
Power source: PSE
```

```
Power priority: unknown
```

```
PD requested power value: 20.0W
```

```
PSE allocated power value: 20.0W
```

```
Switch#
```

**Отображаемые параметры**

<b>Interface</b>	Идентификатор интерфейса PoE.
<b>Power type</b>	Поле типа питания, которое находится в Power via MDI TLV из PSE или PD LLDP-пакета.
<b>Power source</b>	Поле источника питания, которое находится в Power via MDI TLV из PSE или PD LLDP-пакета.
<b>Power priority</b>	Поле приоритета мощности, которое находится в Power via MDI TLV из PSE или PD LLDP-пакета.
<b>PD requested power value</b>	Поле значения мощности, запрашиваемой PD, которое находится в TLV Power via MDI из PSE или PD LLDP-пакета.
<b>PSE allocated power value</b>	Поле значения мощности, выделенной PSE, которое находится в Power via MDI TLV из PSE или PD LLDP-пакета.

## 48-10 show poe power module

Эта команда используется для отображения настроек и фактических значений силовых модулей.

### show poe power module [detail]

#### Параметры

<b>detail</b>	(Опционально) Указывает на отображение более подробной информации о параметрах микросхемы.
---------------	--

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Эта команда отображает подробную информацию о питании и параметры чипа PoE для модулей PoE.

#### Пример

В этом примере показано, как отобразить информацию о мощности системы питания PoE.

```
Switch#show poe power module

Unit  Delivered (W)  Power Budget (W)  Usage-Threshold(%)  Preempt  Trap State
-----
1      0                370               99                  Enabled   Disabled

Switch#
```

#### Отображаемые параметры

<b>Unit</b>	Идентификатор устройства стекирования.
-------------	--



<b>Delivered</b>	Фактическая мощность, подаваемая на PD, в ваттах.
<b>Power budget</b>	Общая мощность, которую может обеспечить устройство, в ваттах.
<b>Usage-Threshold</b>	Порог использования для записи журнала.
<b>Preempt</b>	<b>Enabled:</b> Режим управления питанием - вытеснение политики, PD с высоким приоритетом может вытеснить питание PD с более низким приоритетом. <b>Disabled:</b> Режим управления питанием - "первый обслуживается первым".
<b>Trap State</b>	<b>Enabled (Включено):</b> Ловушка отправляется, когда порог использования PoE превышает указанное значение. <b>Disabled (Отключено):</b> Ловушка не отправляется, когда порог использования PoE превышает указанное значение.

В данном примере показано, как отобразить подробные параметры PoE для устройства 1.

```
Switch#show poe power module unit 1 detail

Unit Delivered(W) Power Budget(W) Usage-Threshold(%) Preempt Trap State
-----
1      0           370           99           Enabled Disabled

PoE system parameters:
Unit Max Ports Device ID SW Version
----
1    24      E111      17

Switch#
```

#### Отображаемые параметры

<b>Max ports</b>	Максимальный номер порта подсистемы PoE.
<b>Device ID</b>	Аппаратная версия чипа PoE.
<b>S/W version</b>	Версия микропрограммы чипа PoE.

## 48-11 poe pd alive

Эта команда используется для включения функции проверки жизни PD для PD, подключенного к порту PoE. Для отключения функции используйте форму **no** этой команды.

```
poe pd alive [{ip IP-ADDRESS | interval INTERVAL-TIME | retry RETRY-COUNT | waiting-time WAITING-TIME | action {reset | notify | both}}]
no poe pd alive [{ip | interval | retry | waiting-time | action}]
```

#### Параметры

<b>ip</b>	(Опционально) Указывает IPv4-адрес целевого PD для системы, выполняющей действие ping.
-----------	--

<b>interval</b>	(Опционально) Указывает интервал, в течение которого система будет отправлять запросы ping для обнаружения целевого PD. Допустимый диапазон - от 10 до 300 секунд.
<b>retry</b>	(Опционально) Указывает количество повторных попыток запросов ping, когда PD не получил ответа. Допустимый диапазон - от 0 до 5.
<b>waiting-time</b>	(Опционально) Указывает время ожидания восстановления PD после перезагрузки. Диапазон допустимых значений составляет от 30 до 300 секунд.
<b>action</b>	(Опционально) Указывает действие системы, когда PD не отвечает на запрос ping. <b>reset</b> - Указывает отключение и последующее включение состояния порта PoE. <b>notify</b> - Указывает отправку журналов и ловушек для уведомления администратора. <b>both</b> - Указывает сначала отправить журнал и ловушку, а затем сбросить состояние порта PoE.

#### По умолчанию

По умолчанию эта функция отключена.

По умолчанию IP-адрес целевого PD не задан.

По умолчанию интервал между запросами ping для системы составляет 30 секунд.

Количество повторных попыток для запросов ping по умолчанию - 2 раза.

Время ожидания по умолчанию для восстановления PD после перезагрузки составляет 90 секунд.

Действие по умолчанию, когда PD не отвечает на запрос ping, - **both**.

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

Эта функция действует только на портах с поддержкой PoE и подачей питания.

Функция проверки работоспособности PD обеспечивает решение для PD-устройства, которое перестает работать или не отвечает на запросы через механизм ping.

Используйте эту команду без параметров, чтобы включить или отключить функцию проверки PD.

По умолчанию IP-адрес целевого PD отсутствует, чтобы система могла выполнить действие ping. IP-адрес целевого PD должен быть настроен с помощью команды **poe pd alive ip** перед выполнением проверки работоспособности PD.

Системе необходимо периодически отслеживать определенный PD с помощью функции ping. При отсутствии ответа система предпринимает одно из действий, настроенных командой **poe pd alive action**. Интервал между повторными попытками может быть настроен командой **poe pd alive interval**.

Система реализует механизм повторных попыток для проверки состояния PD. Система сбросит питание порта PoE после повторной попытки с помощью Ping при отсутствии ответа от PD. Количество повторных попыток может быть настроено командой **poe pd alive retry**.

Если действие **reset** или **both**, системе необходимо подождать, пока PD восстановится после перезагрузки, а затем снова выполнить функцию Ping. Время ожидания восстановления PD после перезагрузки можно настроить с помощью команды **poe pd alive waiting-time**.

Если функция диапазона времени PoE настроена на порту, на котором также включена функция проверки жизни PD, функция диапазона времени имеет более высокий приоритет, и функция проверки жизни PD не будет работать, когда функция диапазона времени PoE все еще активна.



**ПРИМЕЧАНИЕ:** Если PD не поддерживает ICMP, эта функция не сможет нормально работать.

**ПРИМЕЧАНИЕ:** Необходимо правильно настроить параметры IP, чтобы до PD можно было добраться через Ping, иначе эта функция не сможет работать должным образом.

**ПРИМЕЧАНИЕ:** Действие сброса может работать только на PD, подключенном напрямую. Если PD подключен не напрямую, действие сброса может не сработать должным образом.

**ПРИМЕЧАНИЕ:** Если PD, подключенный напрямую, также является PSE, все PD следующего уровня, подключенные к этому PSE, будут заикливаться при каждом действии функции проверки жизни PD при reset или both действиях.

## Пример

В этом примере показано, как включить функцию проверки жизни PoE PD на портах 1 - 2.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/1-2
Switch(config-if-range)#poe pd alive
Switch(config-if-range)#
```

В этом примере показано, как настроить IP-адрес целевого PD.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive ip 192.168.1.150
Switch(config-if)#
```

В этом примере показано, как настроить интервал между запросами ping.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive interval 60
Switch(config-if)#
```

В этом примере показано, как настроить количество повторных попыток для запросов ping.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive retry 4
Switch(config-if)#
```

В этом примере показано, как настроить время ожидания перезагрузки PD.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive waiting-time 120
Switch(config-if)#
```

В этом примере показано, как настроить действие на сброс, когда PD не отвечает.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive action reset
Switch(config-if)#
```

## 48-12 show poe pd alive

Эта команда используется для отображения настроек проверки жизни PD.

**show poe pd alive [interface *INTERFACE-ID* [, | -]]**

### Параметры

<b>interface</b> <i>INTERFACE-ID</i>	Указывает идентификатор интерфейса для отображения.
,	(Опционально) Указывает серию интерфейсов или отделяет диапазон интерфейсов от предыдущего диапазона. Пробел до и после запятой не ставится.
-	(Опционально) Указывает диапазон интерфейсов. Пробел до и после дефиса не ставится.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте эту команду для отображения настроек проверки жизни PD на указанных портах. Если дополнительный параметр не указан, будет отображена информация обо всех портах PoE.

### Пример

В этом примере показано, как отобразить настройки проверки PD alive check на портах 1 - 2.

```
Switch#show poe pd alive interface eth1/0/1-2
```

```
Port ID: eth1/0/1
```

```
-----  
PD Alive State      : Disabled  
PD IP Address       : 0.0.0.0  
Poll Interval       : 30  
Retry Count         : 2  
Waiting Time        : 90  
Action              : both
```

```
Port ID: eth1/0/2
```

```
-----  
PD Alive State      : Disabled  
PD IP Address       : 192.168.1.150  
Poll Interval       : 30  
Retry Count         : 4  
Waiting Time        : 120  
Action              : reset
```

```
Switch#
```

## 49. Команды энергосбережения

### 49-1 dim led

Данная команда используется для отключения индикаторов портов с целью энергосбережения. Используйте форму **no**, чтобы не отключать индикаторы портов с целью энергосбережения.

```
dim led
no dim led
```

#### Параметры

Нет

#### По умолчанию

По умолчанию эта опция отключена.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте данную команду, чтобы отключить индикаторы портов с целью энергосбережения. Используйте форму **no**, чтобы не отключать индикаторы портов с целью энергосбережения. Если данная функция включена, все индикаторы, отображающие статус порта, будут отключены с целью энергосбережения.

#### Пример

В данном примере показано, как отключить индикаторы портов с целью энергосбережения.

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

### 49-2 power-saving

Данная команда используется для включения отдельных функций энергосбережения. Используйте форму **no**, чтобы отключить данные функции.

```
power-saving {link-detection | port-shutdown | dim-led | hibernation}
no power-saving {link-detection | length-detection | port-shutdown | dim-led | hibernation}
```

#### Параметры

<b>link-detection</b>	Укажите, чтобы включать функцию энергосбережения в зависимости от статуса соединения.
<b>port-shutdown</b>	Укажите, чтобы включать функцию энергосбережения по расписанию отключения индикаторов.

<b>dim-led</b>	Укажите, чтобы включить функцию энергосбережения по расписанию отключения порта.
<b>hibernation</b>	Укажите, чтобы включить функцию энергосбережения по расписанию режима сна системы. Данная функция не поддерживается коммутаторами, объединенными в физический стек.

### По умолчанию

По умолчанию данная функция отключена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

С помощью этой команды пользователь может включить или отключить обнаружение соединения, затемнение светодиодов, выключение порта и спящий режим.

Если функция обнаружения соединения включена, устройство может экономить энергию на неактивных портах.

Если включено затемнение светодиодов, устройство будет выключать все светодиоды порта в указанном диапазоне времени для экономии энергии.

Если включено отключение порта, устройство отключит все порты в указанном диапазоне времени для экономии энергии.

Если включен режим гибернации, устройство перейдет в режим гибернации в указанном диапазоне времени для экономии энергии. Этот параметр можно использовать только в том случае, если режим стекирования отключен.

### Пример

В данном примере показано, как отключить порты и перейти в режим сна для энергосбережения.

```
Switch# configure terminal
Switch(config)# power-saving port-shutdown
Switch(config)# power-saving hibernation
Switch(config)#
```

## 49-3 power-saving eee

Данная команда используется для включения функции Energy-Efficient Ethernet (EEE) на определенном порту/портах. Используйте форму **no**, чтобы отключить функцию EEE.

**power-saving eee**  
**no power-saving eee**

### Параметры

Нет

**По умолчанию**

По умолчанию данная функция отключена.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Команда используется для включения или отключения функции Energy-Efficient Ethernet (EEE) на определенном порту/портах. В режиме Power-Saving EEE энергосбережение зависит от использования фактической пропускной способности и будет обеспечено при установленном соединении во время низкого использования трафика пакетов. Если передаваемые данные отсутствуют, на физическом интерфейсе будет включен режим Low Power Idle (LPI).

**Пример**

В данном примере показано, как включить функцию Power-Saving EEE.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# power-saving eee
Switch(config-if)#
```

**49-4 power-saving dim-led time-range**

Данная команда используется для настройки профиля временного диапазона для расписания отключения индикаторов (Dim LED). Используйте форму **no**, чтобы удалить профиль указанного диапазона времени.

**power-saving dim-led time-range** *PROFILE-NAME*  
**no power-saving dim-led time-range** *PROFILE-NAME*

**Параметры**

<i>PROFILE-NAME</i>	Укажите имя профиля временного диапазона, который необходимо настроить. Максимально допустимое количество символов – 32.
---------------------	--

**По умолчанию**

Нет

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Используйте данную команду, чтобы добавить/удалить профиль временного диапазона для расписания отключения индикаторов (Dim LED). Если расписание настроено, все индикаторы порта будут отключены.

**Пример**



В данном примере показано, как добавить профиль временного диапазона для расписания отключения индикаторов.

```
Switch# configure terminal
Switch(config)# power-saving dim-led time-range off-duty
Switch(config)#
```

## 49-5 power-saving hibernation time-range

Данная команда используется для настройки профиля временного диапазона для расписания режима сна системы (Hibernation). Используйте форму **no**, чтобы удалить профиль указанного диапазона времени.

**power-saving hibernation time-range** *PROFILE-NAME*  
**no power-saving hibernation time-range** *PROFILE-NAME*

### Параметры

<i>PROFILE-NAME</i>	Укажите имя профиля временного диапазона, который необходимо настроить. Максимально допустимое количество символов – 32.
---------------------	--

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду, чтобы добавить/удалить профиль временного диапазона для расписания режима сна системы (Hibernation). Когда система входит в режим сна, коммутатор начинает работать в состоянии низкого энергопотребления (режим ожидания). Отключаются все порты и не действуют сетевые функции. Будет работать только консольное соединение через порт RS232. Коммутатор, являющийся питающим устройством Power Sourcing Equipment (PSE), не будет обеспечивать порты электропитанием.

### Пример

В данном примере показано, как добавить профиль временного диапазона для расписания режима сна системы.

```
Switch# configure terminal
Switch(config)# power-saving hibernation time-range off-duty
Switch(config)#
```

## 49-6 power-saving shutdown time-range

Данная команда используется для настройки профиля временного диапазона для расписания отключения порта (Port Shutdown). Используйте форму **no**, чтобы удалить профиль указанного диапазона времени.

**power-saving shutdown time-range** *PROFILE-NAME*  
**no power-saving shutdown time-range** *PROFILE-NAME*

**Параметры**

<i>PROFILE-NAME</i>	Укажите имя профиля временного диапазона, который необходимо настроить. Максимально допустимое количество символов – 32.
---------------------	--

**По умолчанию**

Нет

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Используйте данную команду, чтобы добавить/удалить профиль временного диапазона для расписания отключения порта (Port Shutdown). Если расписание настроено, указанный порт будет отключен.

**Пример**

В данном примере показано, как добавить профиль временного диапазона для расписания отключения порта.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# power-saving shutdown time-range off-duty
Switch(config-if)#
```

**49-7 show power-saving**

Данная команда используется для отображения информации о настройках энергосбережения.

```
show power-saving [link-detection] [length-detection] [dim-led] [port-shutdown] [hibernation]
[eee]
```

**Параметры**

<b>link-detection</b>	(Опционально) Укажите, чтобы отобразить настройки энергосбережения в зависимости от статуса соединения.
<b>dim-led</b>	(Опционально) Укажите, чтобы отобразить настройки энергосбережения за счет отключения индикаторов.
<b>port-shutdown</b>	(Опционально) Укажите, чтобы отобразить настройки энергосбережения за счет отключения порта.
<b>hibernation</b>	(Опционально) Укажите, чтобы отобразить настройки энергосбережения для режима сна.
<b>eee</b>	(Опционально) Укажите, чтобы отобразить настройки энергосбережения для функции EEE.

**По умолчанию**

Нет

## Режим ввода команды

EXEC Mode

## Использование команды

Если ни один из опциональных параметров не указан, будет отображена информация о всех настройках энергосбережения.

## Пример

В данном примере показано, как отобразить информацию о всех настройках энергосбережения.

```
Switch#show power-saving
Function Version: 3.00

Link Detection Power Saving
  State: Disabled

Length Detection Power Saving
  State: Disabled

Scheduled Hibernation Power Saving
  State: Disabled

Administrative Dim-LED
  State: Disabled

Scheduled Dim-LED Power Saving
  State: Disabled

Scheduled Port-shutdown Power Saving
  State: Disabled

EEE_Enabled Ports

Switch#
```

## 50. Команды Protocol Independent

### 50-1 ip route

Эта команда используется для создания записи статического маршрута. Используйте форму **no** этой команды, чтобы удалить запись статического маршрута.

```
ip route NETWORK-PREFIX NETWORK-MASK IP-ADDRESS [primary | backup]
no ip route NETWORK-PREFIX NETWORK-MASK IP-ADDRESS
```

#### Параметры

<i>NETWORK-PREFIX</i>	Укажите сетевой адрес.
<i>NETWORK-MASK</i>	Укажите сетевую маску.
<i>IP-ADDRESS</i>	Укажите IP-адрес следующего узла (Next Hop), который будет использоваться для достижения сети назначения.
<b>primary</b>	(Опционально) Укажите маршрут как основной маршрут к назначению.
<b>backup</b>	(Опционально) Укажите маршрут как резервный маршрут к назначению.

#### По умолчанию

Нет

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Доступны плавающие маршруты. Это означает, что можно создать два маршрута с одним адресом сети назначения, но с разными следующими узлами (Next Hop). Если ни один из параметров (**primary** или **backup**) не указан, роль статического маршрута (основной/резервный) будет назначена автоматически. Основным маршрутом (Primary) является самый приоритетный и всегда используется для продвижения, если находится в активном режиме. Если основной маршрут неактивен, используется резервный маршрут (Backup).

#### Пример

В данном примере показано, как добавить запись статического маршрута. Сетевой адрес – 20.0.0.0/8. Следующий узел – 10.1.1.254.

```
Switch# configure terminal
Switch(config)# ip route 20.0.0.0 255.0.0.0 10.1.1.254
Switch(config)#
```

### 50-2 ipv6 route

Данная команда используется для создания записи статического маршрута IPv6. Используйте форму **no**, чтобы удалить запись статического маршрута IPv6.

```

ipv6 route {default | NETWORK-PREFIX/PREFIX-LENGTH} [INTERFACE-ID] NEXT-HOP-ADDRESS
[primary | backup]
no ipv6 route {default | NETWORK-PREFIX/PREFIX-LENGTH} [INTERFACE-ID] NEXT-HOP-ADDRESS

```

### Параметры

<b>default</b>	Укажите, чтобы добавить или удалить маршрут по умолчанию.
<i>NETWORK-PREFIX/PREFIX-LENGTH</i>	Укажите сетевой префикс и длину префикса статического маршрута.
<i>INTERFACE-ID</i>	(Опционально) Укажите интерфейс передачи для маршрутизации пакетов.
<i>NEXT-HOP-ADDRESS</i>	Укажите IPv6-адрес следующего узла (Next Hop), который будет использоваться для достижения сети назначения. Если адрес является адресом Link-Local, необходимо также указать ID интерфейса.
<b>primary</b>	(Опционально) Укажите маршрут как основной маршрут к назначению.
<b>backup</b>	(Опционально) Укажите маршрут как резервный маршрут к назначению.

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

Доступны плавающие маршруты. Это означает, что можно создать два маршрута с одним адресом сети назначения, но с разными следующими узлами (Next Hop). Если ни один из параметров (**primary** или **backup**) не указан, роль статического маршрута (основной/резервный) будет назначена автоматически. Основной маршрут (Primary) является самым приоритетным и всегда используется для продвижения, если находится в активном режиме. Если основной маршрут неактивен, используется резервный маршрут (Backup).

### Пример

В данном примере показано, как создать статический маршрут для сети, в которой находится прокси-сервер.

```

Switch# configure terminal
Switch(config)# ipv6 route 2001:0101::/32 vlan 1 fe80::0000:00ff:1111:2233
Switch(config)#

```

## 50-3 show ip route

Данная команда используется для отображения записи в таблице маршрутизации.

```

show ip route [IP-ADDRESS [MASK]] | connected | static] | hardware]

```

**Параметры**

<i>IP-ADDRESS</i>	(Опционально) Укажите сетевой адрес, информацию о маршрутизации которого необходимо отобразить.
<i>MASK</i>	(Опционально) Укажите маску подсети для указанной сети.
<b>connected</b>	(Опционально) Указывает отображение маршрута с прямым подключением.
<b>static</b>	(Опционально) Указывает отображение статического маршрута.
<b>hardware</b>	(Опционально) Указывает отображение маршрутов, которые были записаны в микросхему.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте эту команду для отображения лучших маршрутов, которые в настоящее время работают.

**Пример**

В данном примере показано, как отобразить таблицу маршрутизации.

```
Switch#show ip route
Code: C - connected, S - static
      * - candidate default

Gateway of last resort is 10.1.1.254 to network 0.0.0.0

S*   0.0.0.0/0 [1/1] via 10.1.1.254, vlan1
C    10.0.0.0/8 is directly connected, vlan1

Total Entries: 2

Switch#
```

**50-4 show ip route summary**

Данная команда используется для отображения краткой информации о текущих записях маршрутизации.

**show ip route summary**

**Параметры**

Нет

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Данная команда используется для отображения краткой информации о текущих записях маршрутизации.

**Пример**

В данном примере показано, как отобразить краткую информацию о текущих записях маршрутизации.

```
Switch#show ip route summary

Route Source    Networks
Connected       1
Static          0
Total           1

Switch#
```

**50-5 show ipv6 route**

Эта команда используется для отображения записи в таблице маршрутизации.

**show ipv6 route** [[*IPV6-ADDRESS* | *NETWORK-PREFIX/PREFIX-LENGTH* [**longer-prefixes**] | *INTERFACE-ID* | **connected** | **static**] [**database**] | **hardware**]

**Параметры**

<i>IPV6-ADDRESS</i>	(Опционально) Укажите IPv6-адрес, чтобы найти самый длинный префикс соответствующего IPv6-маршрута.
<i>NETWORK-PREFIX</i>	(Опционально) Укажите сетевой адрес, информацию о маршрутизации которого необходимо отобразить.
<i>PREFIX-LENGTH</i>	(Опционально) Укажите длину префикса для указанной сети.
<b>longer-prefixes</b>	(Опционально) Указывает отображение маршрута и всех более конкретных маршрутов.
<i>INTERFACE-ID</i>	(Опционально) Укажите интерфейс, который будет использоваться при отображении.
<b>connected</b>	(Опционально) Указывает отображение маршрута с

	прямым подключением.
<b>static</b>	(Опционально) Указывает отображение статического маршрута.
<b>database</b>	(Опционально) Указывает на отображение всех связанных записей в базе данных маршрутизации, а не только наилучшего маршрута.
<b>hardware</b>	(Опционально) Указывает отображение маршрутов, которые были записаны в микросхеме.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте эту команду для отображения лучших маршрутов, которые в настоящее время работают.

**Пример**

В данном примере показано, как отобразить записи маршрутизации для IPv6.

```
Switch# show ipv6 route

IPv6 Routing Table
Code: C - connected, S - static

C    2000:410:1::/64 [0/1] is directly connected, vlan1
S    2001:0101::/64 [1/1] via fe80::0000:00ff:1111:2233, vlan1
S    2001:0102::/64 [1/1] via fe80::0000:00ff:1111:2233, vlan1

Total Entries: 3 entries, 3 routes

Switch#
```

В данном примере показано отображение записей статической маршрутизации для IPv6.



```
Switch# show ipv6 route static

IPv6 Routing Table
Code: C - connected, S - static

S      2001:0101::/64 [1/1] via fe80::0000:00ff:1111:2233, vlan1
S      2001:0102::/64 [1/1] via fe80::0000:00ff:1111:2233, vlan1

Total Entries: 2 entries, 2 routes

Switch#
```

## 50-6 show ipv6 route summary

Данная команда используется для отображения текущего состояния таблицы маршрутизации IPv6.

### show ipv6 route summary

#### Параметры

Нет

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Если система обслуживания обеспечивает продвижение IPv6-трафика, необходимо проверять таблицу переадресации/маршрутизации для выявления пути трафика, который будет использоваться в сети.

#### Пример

В этом примере показано, как отобразить текущее состояние таблицы маршрутизации IPv6.

```
Switch#show ipv6 route summary

Route Source   Networks
Connected      2
Static         1
SLAAC          0
Total          3

Switch#
```



## 51. Команды качества обслуживания (QOS)

### 51-1 class

Данная команда используется для указания имени карты класса (Class-map) для привязки к политике трафика с дальнейшим переходом в режим Policy-map Configuration Mode. Используйте форму **no**, чтобы удалить описание политики указанного класса.

```
class NAME
no class NAME
class class-default
```

#### Параметры

<i>NAME</i>	Укажите имя карты класса (Class-map) для привязки к политике трафика.
-------------	---

#### По умолчанию

Нет

#### Режим ввода команды

Policy-map Configuration Mode

#### Использование команды

После ввода данной команды будет выполнен вход в режим Policy-map Configuration Mode. Весь трафик, который не соответствует текущему настроенному классу, будет классифицирован как класс по умолчанию (Class-Default). Если указанное имя карты класса не существует, никакой трафик не классифицируется в класс.

#### Пример

В данном примере показано, как настроить карту политики (Policy-map), в которой определены политики для класса «class-dscp-red». Настроенная карта политики – policy1. Все пакеты, соответствующие DSCP-меткам 10, 12 или 14, будут маркированы в качестве DSCP 10 при использовании Single Rate Policer.

```
Switch# configure terminal
Switch(config)# class-map class-dscp-red
Switch(config-cmap)# match ip dscp 10,12,14
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class class-dscp-red
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap-c)# police 1000000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)#
```

### 51-2 class-map

Данная команда используется для входа в режим Class-map Configuration Mode или для создания/изменения карты класса, в которой определены критерии соответствия пакетов. Используйте форму **no**, чтобы удалить существующую карту класса на коммутаторе.

**class-map [match-all | match-any] NAME**  
**no class-map NAME**

### Параметры

<i>NAME</i>	Укажите имя карты класса. Максимально допустимое количество символов – 32.
<b>match-any</b>	(Опционально) Укажите, чтобы критерии соответствия карты класса были оценены на основе логического OR. Если ключевое слово <b>match-all</b> или <b>match-any</b> не указано, по умолчанию будет использовано <b>match-any</b> .
<b>match-all</b>	(Опционально) Укажите, чтобы критерии соответствия карты класса были оценены на основе логического AND. Если ключевое слово <b>match-all</b> или <b>match-any</b> не указано, по умолчанию будет использовано <b>match-any</b> .

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду, чтобы создать или изменить карту класса, в которой определены критерии соответствия пакетов, настраиваемые в режиме Class-map Configuration Mode.

Если для класса настроено несколько команд соответствия, необходимо использовать ключевое слово **match-all** или **match-any**, чтобы указать, на основе чего (логического AND или логического OR) будут оцениваться критерии соответствия.

### Пример

В данном примере показано, как настроить имя карты класса. Настроенное имя – class\_home\_user. Условие соответствия для данной карты класса выполняется, если трафик, соответствующий списку управления доступом «acl\_home\_user» и протоколу IPv6, будет включен в настроенную карту класса «class\_home\_user».

```
Switch# configure terminal
Switch(config)# class-map match-all class_home_user
Switch(config-cmap)# match access-group name acl_home_user
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)#
```

## 51-3 match

Данная команда используется для настройки критериев соответствия для карты класса. Используйте форму **no**, чтобы удалить критерии соответствия.

```
match {access-group name ACCESS-LIST-NAME | cos [inner] COS-LIST | [ip] dscp DSCP-LIST |[ip]
precedence IP-PRECEDENCE-LIST | protocol PROTOCOL-NAME | vlan [inner] VLAN-LIST}
no match {access-group name ACCESS-LIST-NAME | cos [inner] COS-LIST | [ip] dscp DSCP-LIST | [ip]
precedence IP-PRECEDENCE-LIST | protocol PROTOCOL-NAME | vlan [inner] VLAN-ID- LIST}
```

### Параметры

<b>access-group name</b> <i>ACCESS-LIST-NAME</i>	Укажите список доступа в качестве критерия соответствия. Трафик, разрешенный указанным списком доступа, будет классифицирован.
<b>cos [inner]</b> <i>COS-LIST</i>	Укажите значение(я) определенного IEEE 802.1Q в качестве критерия соответствия. Доступный диапазон значений: от 0 до 7. Для перечисления нескольких значений CoS используется запятая, а для обозначения диапазона значений – дефис.
<b>[ip] dscp</b> <i>DSCP-LIST</i>	Укажите значения DSCP-метки в качестве критерия соответствия. Доступный диапазон значений: от 0 до 63. Для перечисления нескольких значений DSCP используется запятая, а для обозначения диапазона значений – дефис. <b>ip</b> – (Опционально) Укажите, чтобы настроить критерий соответствия только для пакетов IPv4. Если не указано, проверка критерий настраивается для пакетов IPv4 и IPv6.
<b>[ip] precedence</b> <i>IP-PRECEDENCE-LIST</i>	Укажите значения приоритета IP в качестве критерия соответствия. Доступный диапазон значений: от 0 до 7. Для перечисления нескольких значений приоритета используется запятая, а для обозначения диапазона значений – дефис. <b>ip</b> – (Опционально) Укажите, чтобы настроить критерий соответствия только для пакетов IPv4. Если не указано, критерий соответствия настраивается для пакетов IPv4 и IPv6. Для пакетов IPv6 приоритетом являются три наиболее значимых бита класса трафика заголовка IPv6.
<b>protocol</b> <i>PROTOCOL-NAME</i>	Укажите имя протокола в качестве критерия соответствия.
<b>vlan [inner]</b> <i>VLAN-LIST</i>	Укажите номер(а) или диапазон номеров идентификации VLAN в качестве критерия соответствия. Доступный диапазон значений: от 1 до 4094. Для перечисления нескольких значений VLAN используется запятая, а для обозначения диапазона значений – дефис.

### По умолчанию

Нет

### Режим ввода команды

Class-map Configuration Mode

### Использование команды

Перед применением данной команды используйте команду **class-map**, чтобы указать имя класса, для которого будут настроены критерии соответствия. Политика обработки данных соответствующих пакетов настраивается в режиме Policy-map Class Configuration Mode.

В списке ниже представлены протоколы, доступные для данной команды:

- **arp** - IP Address Resolution Protocol (ARP)
- **bgp** - Border Gateway Protocol
- **dhcp** - Dynamic Host Configuration
- **dns** - Domain Name Server lookup
- **egp** - Exterior Gateway Protocol
- **ftp** - File Transfer Protocol
- **ip** - IP (version 4)
- **ipv6** - IP (version 6)
- **netbios** – NetBIOS
- **nfs** - Network File System
- **ntp** - Network Time Protocol
- **ospf** - Open Shortest Path First
- **pppoe** - Point-to-Point Protocol over Ethernet
- **rip** - Routing Information Protocol
- **rtsp** - Real-Time Streaming Protocol
- **ssh** - Secured shell
- **telnet** – Telnet
- **tftp** - Trivial File Transfer Protocol

### Пример

В данном примере показано, как настроить карту класса и список доступа, который будет использован в качестве критерия соответствия для данного класса. Имя настроенной карты класса – class-home-user. Имя настроенного списка доступа – acl-home-user.

```
Switch# configure terminal
Switch(config)# class-map class-home-user
Switch(config-cmap)# match access-group name acl-home-user
Switch(config-cmap)#
```

В данном примере показано, как настроить карту класса и значения CoS, которые будут использованы в качестве критериев соответствия для данного класса. Имя настроенной карты класса – cos. Настроенные значения CoS – 1, 2 и 3.

```
Switch# configure terminal
Switch(config)# class-map cos
Switch(config-cmap)# match cos 1,2,3
Switch(config-cmap)#
```

## 51-4 mls qos cos

Данная команда используется для настройки значения CoS по умолчанию для порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
mls qos cos {COS-VALUE | override}
no mls qos cos
```

**Параметры**

<i>COS-VALUE</i>	Укажите значение CoS по умолчанию, которое будет применено к входящим нетегированным пакетам, полученным на порту.
<b>override</b>	Укажите, чтобы отменить CoS пакетов. Для всех полученных на порту пакетов (тегированных и нетегированных) будет применен CoS по умолчанию.

**По умолчанию**

Значение CoS по умолчанию – 0.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Если параметр **override** не указан, для тегированных пакетов применяется CoS, назначенный пакету; для нетегированных пакетов будет применен CoS по умолчанию.

Если параметр **override** указан, для всех полученных на порту пакетов будет применен CoS по умолчанию. Используйте ключевое слово **override**, если все входящие пакеты на определенных портах заслуживают приоритет выше или ниже, чем пакеты, поступающие из других портов. При использовании данной команды, ранее настроенные доверенные DSCP и CoS будут перезаписаны, и все значения CoS входящих пакетов будут изменены на CoS по умолчанию, настроенный в команде **mls qos cos**. Если входящие пакеты тегированные, их значение CoS изменяется на входном порту.

CoS по умолчанию пакетов, поступающих на порт 802.1Q VLAN tunnel, имеет два значения: внутренний CoS, назначенный пакету, и CoS в теге VLAN tunnel передаваемого пакета.

**Пример**

В данном примере показано, как настроить значение CoS по умолчанию на Ethernet-порту 1/0/1. Настроенное значение – 3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# mls qos cos 3
Switch(config-if)#
```

**51-5 mls qos dscp-mutation**

Данная команда используется для привязки карты изменения входящего DSCP (DSCP Mutation) к интерфейсу. Используйте форму **no**, чтобы удалить привязку карты DSCP Mutation к интерфейсу.

```
mls qos dscp-mutation DSCP-MUTATION-TABLE-NAME
no mls qos dscp-mutation
```

**Параметры**

<i>DSCP-MUTATION-TABLE-</i>	Укажите имя таблицы DSCP Mutation без пробелов.
-----------------------------	---

<i>NAME</i>	Максимально допустимое количество символов – 32.
-------------	--

**По умолчанию**

Нет

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Используйте данную команду, чтобы привязать таблицу DSCP Mutation к интерфейсу. Значение DSCP пакета, полученного на интерфейсе, будет изменено с помощью DSCP Mutation. Пакет с новым значением DSCP будет обработан QoS и отправлен из порта коммутатора.

**Пример**

В данном примере показано, как преобразовать значение DSCP и привязать карту изменений внутреннего DSCP (DSCP Mutation) к порту Ethernet 1/0/1. Ранее настроенное значение DSCP – 30. Новое значение – 8. Карта DSCP Mutation – mutemap1.

```
Switch# configure terminal
Switch(config)# mls qos map dscp-mutation mutemap1 30 to 8
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# mls qos dscp-mutation mutemap1
Switch(config-if)#
```

**51-6 mls qos map dscp-cos**

Данная команда используется для привязки DSCP-меток к CoS. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
mls qos map dscp-cos DSCP-LIST to COS-VALUE
no mls qos map dscp-cos DSCP-LIST
```

**Параметры**

<b>dscp-cos DSCP-LIST to COS-VALUE</b>	Укажите список DSCP-меток для привязки к значению CoS. Доступный диапазон значений: от 0 до 63. Несколько DSCP могут быть отделены запятой (,) или дефисом (-). Пробелы до и после дефиса недопустимы.
<i>DSCP-LIST</i>	Укажите диапазон DSCP-меток.

**По умолчанию**

Значение CoS:	0	1	2	3	4	5	6	7
Значение DSCP: 0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63	

**Режим ввода команды**

Interface Configuration Mode



## Использование команды

Данная команда позволяет привязать DSCP-метку доверенного порта DSCP к значению внутреннего CoS. Данное значение CoS будет привязано к очереди CoS на основе CoS в карте очереди, настроенной в команде **priority-queue cos-map**.

## Пример

В данном примере показано, как привязать DSCP к CoS на интерфейсе Ethernet 1/0/6. DSCP-метки 12, 16 и 18 привязаны к CoS 1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/6
Switch(config-if)# mls qos map dscp-cos 12,16,18 to 1
Switch(config-if)#
```

## 51-7 mls qos map dscp-mutation

Данная команда используется для настройки карты DSCP Mutation. Используйте форму **no**, чтобы удалить карту Mutation.

```
mls qos map dscp-mutation MAP-NAME INPUT-DSCP-LIST to OUTPUT-DSCP
no mls qos map dscp-mutation MAP-NAME
```

## Параметры

<i>MAP-NAME</i>	Укажите имя карты DSCP Mutation без пробелов. Максимально допустимое количество символов – 32.
<i>INPUT-DSCP-LIST</i>	Укажите список DSCP, значения которых необходимо «мутировать». Доступный диапазон значений: от 0 до 63. Несколько DSCP могут быть отделены запятой (,) или дефисом (-). Пробелы до и после дефиса недопустимы.
<i>OUTPUT-DSCP</i>	Укажите значение DSCP, которое будет применено после «мутации» Mutation. Доступный диапазон значений: от 0 до 63.

## По умолчанию

Значение DSCP на выходе равно значению DSCP на входе.

## Режим ввода команды

Global Configuration Mode

## Использование команды

Когда пакет принимается интерфейсом, на основе карты мутации DSCP входящий DSCP может быть мутирован в другой DSCP непосредственно перед любыми операциями QoS. Мутация DSCP полезна для интеграции доменов с различными назначениями DSCP.

При настройке именованной карты мутации DSCP обратите внимание на следующее:

- Введите несколько команд для сопоставления дополнительных значений DSCP с измененным значением DSCP.
- Введите отдельную команду для каждого мутированного значения DSCP.

Карта DSCP-CoS и карта DSCP-цвета по-прежнему будут основаны на исходном DSCP пакета. Все последующие операции будут основаны на измененном DSCP.

### Пример

В данном примере показано, как преобразовать DSCP 30 в DSCP 8 и DSCP 20 в DSCP 10. Имя карты Mutation – mutemap1.

```
Switch# configure terminal
Switch(config)# mls qos map dscp-mutation mutemap1 30 to 8
Switch(config)# mls qos map dscp-mutation mutemap1 20 to 10
Switch(config)#
```

## 51-8 mls qos scheduler

Данная команда используется для настройки механизма обслуживания очередей. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
mls qos scheduler {sp | rr | wrr | wdr}
no mls qos scheduler
```

### Параметры

<b>sp</b>	Укажите алгоритм Strict Priority, SP для всех очередей.
<b>rr</b>	Укажите алгоритм Round-Robin, RR для всех очередей.
<b>wrr</b>	Укажите алгоритм Weighted Round-Robin, WRR по числу кадров для всех очередей. Если настроенный вес (Weight) очереди равен нулю, для данной очереди будет включен алгоритм Strict Priority, SP.
<b>wdr</b>	Укажите алгоритм Weighted Deficit Round-Robin, WDRR по длине кадров (Quantum) для очередей всех портов. Если настроенный вес (Weight) очереди равен нулю, для данной очереди включен алгоритм Strict Priority, SP.

### По умолчанию

Алгоритм механизма обслуживания очередей для очереди по умолчанию – WRR.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Укажите алгоритм обслуживания очередей (WRR, SP, RR или WDRR) для выходной очереди. Алгоритм обслуживания очередей для очереди по умолчанию – WRR. WDRR предназначен для набора накопившихся кредитов в очереди передачи в режиме Round-Robin. Изначально для каждой очереди установлен свой счетчик кредита (настроенное значение Quantum). Каждый раз, когда пакет отправляется из очереди CoS, размер пакета вычитается из соответствующего счетчика кредитов, и право на обслуживание переходит к

очереди с более низким CoS. Если счетчик кредитов опускается ниже нуля, очередь не обслуживается до тех пор, пока ее кредиты не будут снова пополнены.

Счетчики кредитов всех очередей CoS при достижении нуля пополняются за один раз.

Обслуживание всех пакетов прекращается, когда их счетчики достигают нуля или становятся меньше нуля, а также после полного осуществления передачи последнего пакета. При выполнении данного условия к каждому счетчику в очереди CoS будет добавлено значение Quantum кредитов. Значение Quantum для каждой очереди может отличаться в зависимости от пользовательских настроек.

Для включения режима Strict Priority для очереди CoS необходимо, чтобы для всех других очередей CoS с более высоким приоритетом также был установлен режим Strict Priority.

WDRR предназначен для передачи разрешенных пакетов в очереди передачи в режиме Round-Robin. Изначально вес каждой очереди установлен на основе настроенного веса. Каждый раз, когда пакет отправляется из очереди CoS с более высоким приоритетом, из соответствующего веса вычитается 1, и право на обслуживание переходит к пакету из очереди CoS с приоритетом ниже предыдущего. Если вес очереди CoS достигает нуля, очередь не обслуживается до тех пор, пока ее вес не будет возобновлен. Вес всех очередей CoS при достижении нуля возобновляется за один раз.

### Пример

В данном примере показано, как настроить алгоритм Strict Priority, SP для очереди.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# mls qos scheduler sp
Switch(config-if)#
```

## 51-9 mls qos trust

Данная команда используется для настройки доверенного статуса (Trust) на порту для поля CoS или DSCP поступающего пакета для последующих QoS-операций. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
mls qos trust {cos | dscp}
no mls qos trust
```

### Параметры

<b>cos</b>	Укажите, чтобы назначить биты CoS поступающих пакетов доверенными для последующих QoS-операций.
<b>dscp</b>	Укажите, чтобы назначить биты ToS/DSCP (если доступны в поступающих пакетах) доверенными для последующих операций. Для не IP-пакетов: доверенной будет назначена информация 2 уровня CoS для классификации трафика.

### По умолчанию

По умолчанию доверенным является CoS.

### Режим ввода команды

Interface Configuration Mode

## Использование команды

После настройки статуса Trust для DSCP на интерфейсе, для последующих QoS-операций DSCP входящих пакетов будет доверенным. Сначала DSCP будет привязан к значению внутреннего CoS, которое в дальнейшем будет использовано для определения очереди CoS. Привязка DSCP к CoS настраивается с помощью команды **mls qos map dscp-cos**. Чтобы настроить CoS в карте очереди, используйте команду **priority-queue cos-map**. Если входящий пакет не IP-пакет, доверенным будет CoS. В передаваемом пакете также будет CoS, полученный в результате привязки DSCP.

После настройки статуса Trust для CoS на интерфейсе, CoS входящих пакетов будет применен в качестве внутреннего CoS и использован для определения очереди CoS. Очередь CoS определяется на основе таблицы соответствия CoS и очереди.

Пакету, прибывшему на порт 802.1Q VLAN tunnel, будет добавлен внешний тег VLAN для передачи через VLAN tunnel. Если на порту настроен статус Trust для CoS, тег внутреннего CoS будет являться CoS пакета и значением CoS во внешнем теге VLAN пакета. Если при вводе команды **mls qos cos** был указан параметр **override**, то внутренним CoS пакета и значением CoS во внешнем теге VLAN пакета будет CoS, настроенный в команде **mls qos cos**. Если на порту настроен статус Trust для DSCP, то внутренним CoS пакета и значением CoS во внешнем теге VLAN пакета будет CoS, полученный в результате привязки DSCP.

## Пример

В данном примере показано, как настроить режим Trust для DSCP на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)#
```

## 51-10 policy-map

Данная команда используется для входа в режим Policy-map Configuration Mode и создания/изменения карты политики, которая может быть привязана к одному или нескольким интерфейсам в качестве политики обслуживания. Используйте форму **no**, чтобы удалить карту политики.

```
policy-map NAME
no policy-map NAME
```

### Параметры

<i>NAME</i>	Укажите имя карты политики. Максимально допустимое количество символов – 32.
-------------	--

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду, чтобы войти в режим Policy-map Configuration Mode и настроить/изменить политику для класса трафика. Одна карта политики может быть привязана к нескольким интерфейсам одновременно. Предыдущие привязки карты политики будут перезаписаны новыми.

Карты политики содержат классы трафика, которые включают в себя одну или более команд для соответствия пакетов и для организации пакетов в группы на основе типа протокола или приложения.

### Пример

В данном примере показано, как создать карту политики под именем «policy» и настроить для нее две политики класса. Первый класс «class1» указывает политику для трафика, соответствующего списку управления доступом (ACL) «acl\_rd». Второй класс является классом по умолчанию «class-default». В данный класс включены пакеты, которые не соответствуют настроенным классам.

```
Switch# configure terminal
Switch(config)# class-map class1
Switch(config-cmap)# match access-group name acl_rd
Switch(config-cmap)# exit
Switch(config)# policy-map policy
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 46
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set ip dscp 00
Switch(config-pmap-c)#
```

## 51-11 priority-queue cos-map

Данная команда используется для привязки CoS к карте очереди. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
priority-queue cos-map QUEUE-ID COS1 [COS2 [COS3 [COS4 [COS5 [COS6 [COS7 [COS8]]]]]]]
no priority-queue cos-map
```

### Параметры

<i>QUEUE-ID</i>	Укажите ID очереди, к которой будет привязан CoS.
<i>COS1</i>	Укажите значение CoS для привязки. Доступный диапазон значений: от 0 до 7.
<i>COS2 ... COS8</i>	(Опционально) Укажите значение CoS для привязки. Доступный диапазон значений: от 0 до 7.

### По умолчанию

Привязка приоритета CoS к очереди по умолчанию: 0 к 2, 1 к 0, 2 к 1, 3 к 3, 4 к 4, 5 к 5, 6 к 6, 7 к 7.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Полученному пакету присваивается внутренний CoS, который используется для выбора очереди передачи на основе привязки карты CoS к карте очереди. Чем выше значение CoS очереди, тем выше приоритет.

### Пример

В данном примере показано, как привязать приоритет CoS 3, 5 и 6 к очереди 2.

```
Switch# configure terminal
Switch(config)# priority-queue cos-map 2 3 5 6
Switch(config)#
```

## 51-12 queue rate-limit

Данная команда используется для указания/изменения полосы пропускания (Bandwidth), предназначенной для очереди. Используйте форму **no**, чтобы удалить полосу пропускания, предназначенную для очереди.

```
queue QUEUE-ID rate-limit {MIN-BANDWIDTH-KBPS | percent MIN-PERCENTAGE} {MAX-BANDWIDTH-KBPS | percent MAX PERCENTAGE}
no queue QUEUE-ID rate-limit
```

### Параметры

<i>QUEUE-ID</i>	Укажите ID очереди, для которой необходимо настроить минимальную разрешенную и максимальную полосу пропускания.
<i>MIN-BANDWIDTH-KBPS</i>	Укажите минимальную разрешенную полосу пропускания в Кбит/с для указанной очереди.
<i>MAX-BANDWIDTH-KBPS</i>	Укажите максимальную полосу пропускания в Кбит/с для указанной очереди.
<i>MIN-PERCENTAGE</i>	Укажите минимальную полосу пропускания в процентах. Доступный диапазон значений: от 1 до 100.
<i>MAX PERCENTAGE</i>	Укажите максимальную полосу пропускания в процентах. Доступный диапазон значений: от 1 до 100.

### По умолчанию

Нет

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Используйте данную команду, чтобы настроить минимальную и максимальную полосу пропускания для определенной очереди. Если минимальная полоса пропускания настроена, пакет, передаваемый из данной очереди, гарантирован. Если настроена максимальная полоса пропускания, пакеты, передаваемые из данной очереди, не могут превышать максимальную полосу пропускания, даже если полоса пропускания доступна.

Значение всей минимальной полосы пропускания должно быть меньше 75 процентов полосы пропускания интерфейса. Для очереди с наивысшим приоритетом настройка минимальной разрешенной полосы

пропускания необязательна, так как трафик данной очереди обслуживается в первую очередь, если все очереди соответствуют заданной минимальной полосе пропускания.

Данная команда используется для настройки физического порта, для port-channel команда недоступна. На физических портах невозможна настройка минимальной разрешенной полосы пропускания одного CoS.

### Пример

В данном примере показано, как настроить полосу пропускания очереди для интерфейса Ethernet 1/0/1. Для очереди 1 «queue 1» настроены минимальная разрешенная полоса пропускания 100 Кбит/с и максимальная полоса пропускания 2000 Кбит/с. Для очереди 2 «queue 2» настроены минимальная разрешенная полоса пропускания 10% и максимальная полоса пропускания 50%.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# queue 1 rate-limit 100 2000
Switch(config-if)# queue 2 rate-limit percent 10 percent 50
Switch(config-if)#
```

## 51-13 rate-limit {input | output}

Данная команда используется для настройки значений ограничения полосы пропускания для входящего и исходящего трафика на интерфейсе. Используйте форму **no**, чтобы отменить ограничение полосы пропускания.

**rate-limit {input | output} {NUMBER-KBPS | percent PERCENTAGE} [BURST-SIZE]**  
**no rate-limit {input | output}**

### Параметры

<b>input</b>	Укажите ограничение полосы пропускания для входящих пакетов.
<b>output</b>	Укажите ограничение полосы пропускания для исходящих пакетов.
<i>NUMBER-KBPS</i>	Укажите ограничение максимальной полосы пропускания в Кбит/с.
<i>PERCENTAGE</i>	Укажите для настройки ограничения в процентах. Доступный диапазон значений: от 1 до 100.
<i>BURST-SIZE</i>	(Опционально) Укажите ограничение для трафика всплеска (Burst). Единица измерения – Кбайт.

### По умолчанию

Нет

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Настроенное ограничение не должно превышать максимальную скорость на указанном интерфейсе. Если полученный трафик превышает настроенное ограничение входящей полосы пропускания, отправляются кадры PAUSE или кадры Flow Control (управления потоком).

### Пример

В данном примере показано, как настроить ограничения максимальной полосы пропускания на интерфейсе Ethernet 1/0/5. Настроенные ограничения входящей полосы пропускания: 2000 Кбит/с и 4096 Кбайт для трафика всплеска (Burst).

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/5
Switch(config-if)# rate-limit input 2000 4096
Switch(config-if)#
```

## 51-14 service-policy

Данная команда используется для привязки карты политики к типу input или output на интерфейсе. Используйте форму **no**, чтобы удалить политику обслуживания из входящего интерфейса (input).

```
service-policy input NAME
no service-policy input
```

### Параметры

<b>input</b>	Укажите, чтобы привязать карту политики к входящему потоку на интерфейсе.
<i>NAME</i>	Укажите имя карты политики обслуживания. Максимально допустимое количество символов – 32.

### По умолчанию

Нет

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Используйте эту команду, чтобы прикрепить к интерфейсу не более одной карты политики для входного типа. Эта политика прикрепляется к интерфейсу для агрегации и управляет количеством или скоростью пакетов. Пакет, поступающий на порт, будет обрабатываться на основе политики обслуживания, прикрепленной к интерфейсу.

### Пример

В этом примере показано, как создать карту политики "cust1-class" и прикрепить ее к порту 1 для входящего трафика.



```
Switch#configure terminal
Switch(config)#policy-map cust1-classes
Switch(config-pmap)#exit
Switch(config)#interface eth1/0/1
Switch(config-if)#service-policy input cust1-classes
Switch(config-if)#
```

## 51-15 set

Данная команда используется для настройки полей нового приоритета (Precedence), DSCP и CoS исходящего пакета. Также возможна настройка очереди CoS для пакета.

```
set {[ip] precedence PRECEDENCE | [ip] dscp DSCP | cos COS | cos-queue COS-QUEUE}
no set {[ip] precedence PRECEDENCE | [ip] dscp DSCP | cos COS | cos-queue COS-QUEUE}
```

### Параметры

<b>precedence</b> <i>PRECEDENCE</i>	Укажите новый приоритет пакета. Доступный диапазон значений: от 0 до 7. Если указано ключевое слово <b>ip</b> , будет отмечен приоритет IPv4. Если не указано, будут отмечены приоритеты IPv4 и IPv6. Для пакетов IPv6 приоритетом являются три наиболее значимых бита класса трафика заголовка IPv6. Настройка приоритета не повлияет на выбор очереди CoS.
<b>dscp</b> <i>DSCP</i>	Укажите новый DSCP пакета. Доступный диапазон значений: от 0 до 63. Если указано ключевое слово <b>ip</b> , будет отмечен IPv4 DSCP. Если не указано, будут отмечены IPv4 и IPv6 DSCP. Настройка DSCP не повлияет на выбор очереди CoS.
<b>cos</b> <i>COS</i>	Укажите новое значение CoS пакета. Доступный диапазон значений: от 0 до 7. Настройка CoS не повлияет на выбор очереди CoS.
<b>cos-queue</b> <i>COS-QUEUE</i>	Укажите очередь CoS для пакетов. Новое значение очереди CoS заменит первоначальное. Очередь CoS не будет назначена, если карта политики привязана к исходящему потоку на интерфейсе.

### По умолчанию

Нет

### Режим ввода команды

Policy-map Class Configuration Mode

### Использование команды

Используйте данную команду, чтобы настроить новое значение полей приоритета (Precedence), DSCP и CoS соответствующих пакетов. Используйте команду **set cos-queue**, чтобы сразу же назначить очередь CoS для соответствующих пакетов.

Возможна настройка нескольких команд для класса, если они не конфликтуют.

Команда **set dscp** не повлияет на выбор очереди CoS. Команда **set cos-queue** не изменит поле CoS исходящего пакета. Команды **police** и **set** могут быть использованы для одного класса. Команда **set** применяется к пакетам всех цветов.

### Пример

В этом примере показано, как настроить карту политики "policy1" с политикой для класса class1. Пакеты, включенные в класс class1, будут иметь DSCP 10.

```
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap-c)#
```

## 51-16 show class-map

Данная команда используется для отображения настроек карты класса.

**show class-map [NAME]**

### Параметры

<i>NAME</i>	(Опционально) Укажите имя карты класса. Максимально допустимое количество символов – 32.
-------------	--

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте данную команду, чтобы отобразить все карты класса и их критерии соответствия.

### Пример

В данном примере показано, как настроены две карты класса. Пакеты, соответствующие списку доступа «acl\_home\_user», принадлежат настроенному классу «с3». IP-пакеты принадлежат настроенному классу «с2».

```
Switch# show class-map

Class Map match-any class-default
  Match any

Class Map match-all c2
  Match protocol ip

Class Map match-all c3
  Match access-group acl_home_user

Switch#
```

## 51-17 show mls qos interface

Данная команда используется для отображения настроек уровня QoS на указанном интерфейсе.

**show mls qos interface** *INTERFACE-ID* [, | -] {**cos** | **scheduler** | **trust** | **rate-limit** | **queue-rate-limit** | **dscp-mutation** | **map dscp-cos**}

### Параметры

<b>interface</b> <i>INTERFACE-ID</i>	Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
<b>cos</b>	Укажите, чтобы отобразить CoS по умолчанию.
<b>scheduler</b>	Укажите, чтобы отобразить настройки механизма обслуживания очереди передачи.
<b>trust</b>	Укажите, чтобы отобразить статус Trust порта.
<b>rate-limit</b>	Укажите, чтобы отобразить ограничение полосы пропускания, настроенной для порта.
<b>queue-rate-limit</b>	Укажите, чтобы отобразить ограничение полосы пропускания, настроенной для очереди.
<b>dscp-mutation</b>	Укажите, чтобы отобразить карту DSCP Mutation, привязанную к интерфейсу.
<b>map dscp-cos</b>	Укажите, чтобы отобразить привязку DSCP к CoS.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Данная команда используется для отображения настроек уровня QoS на указанном интерфейсе.

**Пример**

В данном примере показано, как отобразить CoS по умолчанию для интерфейсов от Ethernet 1/0/2 до Ethernet 1/0/5.

```
Switch# show mls qos interface ethernet 1/0/2-5 cos
```

Interface	CoS	Override
eth1/0/2	3	Yes
eth1/0/3	4	No
eth1/0/4	4	No
eth1/0/5	3	No

```
Switch#
```

В данном примере показано, как отобразить статус Trust порта для интерфейсов от Ethernet 1/0/2 до Ethernet 1/0/5.

```
Switch# show mls qos interface ethernet 1/0/2-1/0/5 trust
```

Interface	Trust State
eth1/0/2	trust DSCP
eth1/0/3	trust CoS
eth1/0/4	trust DSCP
eth1/0/5	trust CoS

```
Switch#
```

В данном примере показано, как отобразить настройки механизма обслуживания очередей для интерфейсов Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch# show mls qos interface ethernet 1/0/1-1/0/2 scheduler
```

Interface	Scheduler Method
eth1/0/1	sp
eth1/0/2	wrr

```
Switch#
```

В данном примере показано, как отобразить карты DSCP Mutation, которые привязаны к интерфейсам Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch# show mls qos interface ethernet 1/0/1-2 dscp-mutation
```

Interface	DSCP Mutation Map
eth1/0/1	Mutate Map 1
eth1/0/2	Mutate Map 2

```
Switch#
```

В данном примере показано, как отобразить ограничение полосы пропускания для интерфейсов от Ethernet 1/0/1 до Ethernet 1/0/4.

```
Switch# show mls qos interface ethernet 1/0/1-4 rate-limit
```

Interface	Rx Rate	Tx Rate	Rx Burst	Tx Burst
eth1/0/1	1000 kbps	No Limit	64 kbyte	No Limit
eth1/0/2	No Limit	2000 kbps	No Limit	2000 kbyte
eth1/0/3	10%(100000 kbps)	20%(200000 kbps)	64 kbyte	64 kbyte
eth1/0/4	2%	2000 kbps	64 kbyte	64 kbyte

```
Switch#
```

В данном примере показано, как отобразить ограничение полосы пропускания CoS для интерфейсов Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch# show mls qos interface ethernet 1/0/1-2 queue-rate-limit
```

```
eth1/0/1
QID  Min Bandwidth  Max Bandwidth
-----
0      -              -
1      16 kbps        10%(100000 kbps)
2      32 kbps        -
3      2%             50%
4      64 kbps        -
5      64 kbps        -
6      32 kbps        -
7      -              128 kbps
```

```
eth1/0/2
QID  Min Bandwidth  Max Bandwidth
-----
0      -              -
1      16 kbps        -
2      32 kbps        -
3      32 kbps        -
4      64 kbps        -
5      64 kbps        -
6      32 kbps        -
7      -              128 kbps
```

```
Switch#
```

В данном примере показано, как отобразить привязку DSCP к CoS для интерфейса Ethernet 1/0/1.

```
Switch# show mls qos interface ethernet 1/0/1 map dscp-cos

eth1/0/1
0  1  2  3  4  5  6  7  8  9
-----
00  00 00 00 00 00 00 00 00 01 01
10  01 01 01 01 01 01 01 02 02 02
20  02 02 02 02 03 03 03 03 03 01
30  03 03 04 04 04 04 04 04 04 04
40  05 05 05 05 05 05 05 05 06 06
50  06 06 06 06 06 06 07 07 07 07
60  07 07 07 07

Switch#
```

## 51-18 show mls qos map dscp-mutation

Данная команда используется для отображения настроек карты QoS DSCP Mutation.

**show mls qos maps dscp-mutation [MAP-NAME]**

### Параметры

<i>MAP-NAME</i>	(Опционально) Укажите имя карты DSCP Mutation, которую необходимо отобразить.
-----------------	---

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Данная команда используется для отображения настроек карты QoS DSCP Mutation.

### Пример

В данном примере показано, как отобразить карту DSCP Mutation глобально.

```

Switch#show mls qos map dscp-mutation

DSCP Mutation: mutation
Attaching interface:
  eth1/0/2-1/0/3,1/0/8-1/0/10

  0  1  2  3  4  5  6  7  8  9
-----
00  00 10 02 10 04 05 06 07 08 09
10  10 11 12 13 14 15 16 17 18 19
20  20 21 22 23 24 25 26 27 28 29
30  30 31 32 33 34 35 36 37 38 39
40  40 41 42 43 44 45 46 47 48 49
50  50 51 52 53 54 55 56 57 58 59
60  60 61 62 63

Switch#

```

## 51-19 show mls qos queueing

Данная команда используется для отображения информации об очередях QoS и настроек веса (Weight) для разных алгоритмов обслуживания очередей на определенном интерфейсе или интерфейсах.

**show mls qos queueing [interface *INTERFACE-ID* [, | -]]**

### Параметры

<b>interface</b> <i>INTERFACE-ID</i>	(Опционально) Укажите ID интерфейса, для которого необходимо отобразить информацию о настройках веса (Weight) разных алгоритмов обслуживания очередей.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте эту команду для отображения информации об очередях QoS и конфигурации веса для различных алгоритмов планировщика на указанном(ых) интерфейсе(ах). Если параметр не указан, будет отображена общесистемная карта CoS к ID очереди.

Режим Scheduling, который настроен при помощи команды **mls qos scheduler**, определяет, какие настройки будут действовать для веса. Используйте команду **show mls qos interface scheduler**, чтобы отобразить настроенный алгоритм обслуживания очередей на интерфейсе.

### Пример

В данном примере показано, как отобразить информацию об очередях QoS.

```
Switch#show mls qos queueing

CoS-queue map:
  CoS   QID
  ---   ---
    0     2
    1     0
    2     1
    3     3
    4     4
    5     5
    6     6
    7     7

Switch#
```

В данном примере показано, как отобразить настройки веса для разных алгоритмов обслуживания очередей на интерфейсе Ethernet 1/0/3.



```
Switch# show mls qos queueing interface eth1/0/3
```

```
wrr bandwidth weights:
```

QID	Weights
---	-----
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

```
wrrr bandwidth weights:
```

QID	Quantum
---	-----
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

```
Switch#
```

## 51-20 show policy-map

Данная команда используется для отображения настроек карты политики.

```
show policy-map [POLICY-NAME] interface INTERFACE-ID
```

### Параметры

<i>POLICY-NAME</i>	(Опционально) Укажите имя карты политики. Если не указано, будут отображены все карты политики.
<b>interface</b> <i>INTERFACE-ID</i>	(Опционально) Укажите модуль и номер порта.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте эту команду для отображения политики классов, настроенной для карты политики.

### Пример

В этом примере показано, как отобразить политику классов, настроенную для карты политики.

```
Switch#show policy-map
Policy Map cust1-classes
Class Map gold

Switch#
```

## 51-21 wdr-queue bandwidth

Данная команда используется для настройки значений Quantum для очередей, обслуживаемых механизмом WDRR. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
wdr-queue bandwidth QUANTUM1...QUANTUM8
no wdr-queue bandwidth
```

### Параметры

<i>QUANTUM1...QUANTUM8</i>	Определяет значение кванта (счетчик длины кадра) для каждой из восьми очередей квантования, используемых в планировании WDRR. Диапазон значений квантования - от 0 до 127.
----------------------------	--

### По умолчанию

Значение Quantum для каждой очереди по умолчанию – 1.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Чтобы использовать данную команду, необходимо перейти в режим обслуживания очередей WDRR с помощью команды **mls qos scheduler wdr**.

### Пример

В данном примере показано, как настроить значения Quantum для очередей в режиме обслуживания очередей WDRR на интерфейсе Ethernet 1/0/1. Для очереди 0 настроено значение 1, для очереди 1 – 2, для очереди 2 – 3, для очереди 3 – 4, для очереди 5 – 6, для очереди 6 – 7 и для очереди 7 – 8.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# mls qos scheduler wrr
Switch(config-if)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
Switch(config-if)#
```

## 51-22 wrr-queue bandwidth

Данная команда используется для настройки веса (Weight) для очередей, обслуживаемых механизмом WRR. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
wrr-queue bandwidth WEIGHT1...WEIGHT8
no wrr-queue bandwidth
```

### Параметры

<i>WEIGHT1...WEIGHT8</i>	Указывает значение веса (количество кадров) для каждой из восьми весовых очередей, используемых в планировании WRR. Диапазон значений веса составляет от 0 до 127.
--------------------------	--

### По умолчанию

Значение веса для параметров от *WEIGHT1* до *WEIGHT7* по умолчанию – 1.  
Значение веса для *WEIGHT8* по умолчанию – 0.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Чтобы использовать данную команду, необходимо перейти в режим обслуживания очередей WRR с помощью команды **mls qos scheduler wrr**. При обслуживании Expedited Forwarding (EF) для очереди с наивысшим приоритетом всегда используется политика Per-hop Behavior (PHB) EF и настраивается режим обслуживания очередей по строгому приоритету (Strict Priority). При использовании Differentiate Service необходимо, чтобы вес последней очереди был равен нулю.

### Пример

В данном примере показано, как настроить значения веса (Weight) очередей в режиме обслуживания очередей WRR на интерфейсе Ethernet 1/0/1. Для очереди 0 настроено значение 1, для очереди 1 – 2, для очереди 2 – 3, для очереди 3 – 4, для очереди 4 – 5, для очереди 5 – 6, для очереди 6 – 7 и для очереди 7 – 8.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# mls qos scheduler wrr
Switch(config-if)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
Switch(config-if)#
```

## 52. Команды Remote Network MONitoring (RMON)

### 52-1 rmon collection stats

Данная команда используется для включения статистики RMON на настраиваемом интерфейсе. Используйте форму **no**, чтобы отключить статистику.

```
rmon collection stats INDEX [owner NAME]
no rmon collection stats INDEX
```

#### Параметры

<i>INDEX</i>	Укажите индекс таблицы RMON. Доступный диапазон значений: от 1 до 65535.
<i>owner NAME</i>	Укажите имя владельца. Максимально допустимое количество символов в строке – 127.

#### По умолчанию

По умолчанию данная функция отключена.

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

Номер записи группы статистики RMON является динамическим. Соответствующая запись в таблице будет доступна только на интерфейсе с включенной статистикой RMON.

#### Пример

В данном примере показано, как настроить запись статистики RMON на интерфейсе Ethernet 1/0/2. Индекс – 65. Имя владельца – guest.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# rmon collection stats 65 owner guest
Switch(config-if)#
```

### 52-2 rmon collection history

Данная команда используется для включения сбора истории статистики RMON MIB на настраиваемом интерфейсе. Используйте форму **no**, чтобы отключить сбор истории статистики на интерфейсе.

```
rmon collection history INDEX [owner NAME] [buckets NUM] [interval SECONDS]
no rmon collection history INDEX
```

#### Параметры

<i>INDEX</i>	Укажите индекс таблицы RMON. Доступный диапазон
--------------	---

	значений: от 1 до 65535.
<b>owner NAME</b>	Укажите имя владельца. Максимально допустимое количество символов в строке – 127.
<b>buckets NUM</b>	Укажите количество ячеек для сбора истории по группе статистики RMON. Доступный диапазон значений: от 1 до 65535. Если не указано, используется значение по умолчанию – 50.
<b>interval SECONDS</b>	Укажите время в секундах для каждого цикла опроса (Polling Cycle). Доступный диапазон значений: от 1 до 3600.

**По умолчанию**

По умолчанию данная функция отключена.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Номер записи группы статистики RMON является динамическим. Соответствующая запись в таблице будет доступна только на интерфейсе с включенной статистикой RMON. Настроенный интерфейс становится источником данных для созданной записи.

**Пример**

В данном примере показано, как включить сбор истории по группе статистики RMON MIB на интерфейсе Ethernet 1/0/8.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/8
Switch(config-if)# rmon collection history 101 owner it@domain.com interval 2000
Switch(config-if)#
```

**52-3 rmon alarm**

Данная команда используется для настройки записи уровня alarm (тревога) для мониторинга интерфейса. Используйте форму **no**, чтобы удалить запись уровня alarm.

**rmon alarm INDEX VARIABLE INTERVAL {delta | absolute} rising-threshold VALUE [RISING-EVENT-NUMBER] falling-threshold VALUE [FALLING-EVENT-NUMBER] [owner STRING]**  
**no rmon alarm INDEX**

**Параметры**

<b>INDEX</b>	Укажите индекс alarm. Доступный диапазон значений: от 1 до 65535.
<b>VARIABLE</b>	Укажите идентификатор объекта переменной для выборки.
<b>INTERVAL</b>	Укажите интервал в секундах для выборки переменной и проверки соответствия пороговых значений. Доступный диапазон значений: от 1 до 2147483647.
<b>delta</b>	Укажите для мониторинга дельты (Delta) двух

	последовательных значений выборки.
<b>absolute</b>	Укажите для мониторинга абсолютного значения выборки
<b>rising-threshold VALUE</b>	Укажите верхнее пороговое значение. Доступный диапазон значений: от 0 до 2147483647.
<b>RISING-EVENT-NUMBER</b>	(Опционально) Укажите индекс записи события, при котором превышено заданное верхнее пороговое значение. Доступный диапазон значений: от 1 до 65535. Если не указано, никакие действия при превышении верхнего порогового значения не будут применены.
<b>falling-threshold VALUE</b>	Укажите нижнее пороговое значение. Доступный диапазон значений: от 0 до 2147483647.
<b>FALLING-EVENT-NUMBER</b>	(Опционально) Укажите индекс записи события, при котором достигнуто заданное нижнее пороговое значение. Доступный диапазон значений: от 1 до 65535. Если не указано, никакие действия при достижении нижнего порогового значения не будут применены.
<b>owner STRING</b>	Указывает строку владельца. Максимальная длина - 127.

**По умолчанию**

Нет

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

После настройки RMON alarm будут периодически производится выборки переменных, значения которых будут проверены на соответствие настроенным пороговым значениям.

**Пример**

В данном примере показано, как настроить запись уровня alarm для мониторинга интерфейса.

```
Switch# configure terminal
Switch(config)# rmon alarm 783 1.3.6.1.2.1.2.2.1.12.6 30 delta rising-threshold 20 1 falling-
threshold 10 1 owner Name
Switch(config)#
```

**52-4 rmon event**

Данная команда используется для настройки записи события. Используйте форму **no**, чтобы удалить запись события.

```
rmon event INDEX [log] [[trap COMMUNITY] [owner NAME] [description TEXT]
no rmon event INDEX
```

**Параметры**

<b>INDEX</b>	Укажите индекс записи события. Доступный диапазон значений: от 1 до 65535.
--------------	--

<b>log</b>	(Опционально) Укажите, чтобы генерировать сообщения в системном журнале для уведомлений.
<b>trap</b> <i>COMMUNITY</i>	(Опционально) Укажите, чтобы генерировать сообщения SNMP trap для уведомлений. Максимально допустимая длина – 127.
<b>owner</b> <i>NAME</i>	Укажите имя владельца. Максимально допустимая длина – 127.
<b>description</b> <i>TEXT</i>	(Опционально) Укажите описание для записи события RMON. Максимально допустимое количество символов в строке – 127.

**По умолчанию**

Нет

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Если указан параметр **log**, а **trap** не указан, при возникновении события генерируется запись в журнале. Если указан параметр **trap**, а **log** не указан, при возникновении события генерируется SNMP-уведомление.

Если указаны оба параметра (**log** и **trap**), при возникновении события генерируется и запись в журнале, и SNMP-уведомление.

**Пример**

В данном примере показано, как настроить генерирование записи в журнале при возникновении события. Индекс – 13.

```
Switch# configure terminal
Switch(config)# rmon event 13 log owner it@domain.com description ifInNUcastPkts is too much
Switch(config)#
```

**52-5 show rmon alarm**

Данная команда используется для отображения конфигурации alarm.

```
show rmon alarm
```

**Параметры**

Нет

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

### Использование команды

Используйте данную команду, чтобы отобразить таблицу RMON alarm.

### Пример

В данном примере показано, как отобразить таблицу RMON alarm.

```
Switch# show rmon alarm

Alarm index 23, owned by IT
  Monitors OID: 1.3.6.1.2.1.2.2.1.10.1
  every 120 second(s)
  Taking delta samples, last value was 2500
  Rising threshold is 2000, assigned to event 12
  Falling threshold is 1100, assigned to event 12
  On startup enable rising or falling alarm

Switch#
```

## 52-6 show rmon events

Данная команда используется для отображения таблицы событий RMON.

### show rmon events

#### Параметры

Нет

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

### Использование команды

Используйте данную команду, чтобы отобразить таблицу событий RMON.

### Пример

В данном примере показано, как отобразить таблицу событий RMON.



```
Switch# show rmon events

Event 1, owned by manager1
  Description is Errors
  Event trigger action: log & trap sent to community manager
  Last triggered time: 13:12:15, 2013-03-02

Event 2, owned by manager2
  Description is Errors
  Event trigger action: log & trap
  Last triggered time:

Switch#
```

## 62-7 show rmon history

Данная команда используется для отображения информации об истории статистики RMON.

### show rmon history

#### Параметры

Нет

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте данную команду, чтобы отобразить историю статистики для всех настроенных записей.

#### Пример

В данном примере показано, как отобразить историю статистики RMON Ethernet.

```
Switch# show rmon history

Index 23, owned by Manager, Data source is eth4/0/2
Interval: 30 seconds
Requested buckets: 50, Granted buckets: 50
Sample #1
  Received octets: 303595962, Received packets: 357568
  Broadcast packets: 3289, Multicast packets: 7287
  Estimated utilization: 19
  Undersized packets: 213, Oversized packets: 24
  Fragments: 2, Jabbers: 1
  CRC alignment errors: 0, Collisions: 0
Drop events : 0
Sample #2
  Received octets: 303596354, Received packets: 357898
  Broadcast packets: 3329, Multicast packets: 7337
  Estimated utilization: 19
  Undersized packets: 213, Oversized packets: 24
  Fragments: 2, Jabbers: 1
  CRC alignment errors: 0, Collisions: 0
Drop events : 0

Switch#
```

## 52-8 show rmon statistics

Данная команда используется для отображения статистики RMON Ethernet.

### show rmon statistics

#### Параметры

Нет

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте данную команду, чтобы отобразить статистику для всех настроенных записей.

#### Пример

В данном примере показано, как отобразить статистику RMON.

```
Switch# show rmon statistics

Index 32, owned by it@domain.com, Data Source is eth4/0/3
Received Octets : 234000, Received packets : 9706
Broadcast packets: 2266, Multicast packets: 192
Undersized packets: 213, Oversized packets: 24
Fragments: 2, Jabbers: 1
CRC alignment errors: 0, Collisions: 0
Drop events : 0
Packets in 64 octets: 256, Packets in 65-127 octets : 236
Packets in 128-255 octets : 129, Packets in 256-511 octets : 10
Packets in 512-1023 octets : 38, Packets in 1024-1518 octets : 2200

Switch#
```

## 52-9 snmp-server enable traps rmon

Данная команда используется для включения отправки RMON trap. Используйте форму **no**, чтобы отключить отставку RMON trap.

```
snmp-server enable traps rmon [rising-alarm | falling-alarm]
no snmp-server enable traps rmon [rising-alarm | falling-alarm]
```

### Параметры

<b>rising-alarm</b>	(Опционально) Укажите, чтобы настроить отставку trap, уведомляющих о поднятии тревоги.
<b>falling-alarm</b>	(Опционально) Укажите, чтобы настроить отставку trap, уведомляющих об отмене тревоги.

### По умолчанию

По умолчанию данная функция отключена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду, чтобы включить/отключить отставку RMON trap.

### Пример

В данном показано, как включить отставку RMON trap, уведомляющих о поднятии и об отмене тревоги.

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

## 53. Команды Router Advertisement (RA) Guard

### 53-1 ipv6 nd rguard policy

Данная команда используется для создания политики Router Advertisement (RA) Guard Policy и для входа в режим RA Guard Policy Configuration Mode. Используйте форму **no**, чтобы удалить политику RA Guard Policy.

```
ipv6 nd rguard policy POLICY-NAME
no ipv6 nd rguard policy POLICY-NAME
```

#### Параметры

<i>POLICY-NAME</i>	Укажите имя политики IPv6 RA Guard Policy.
--------------------	--

#### По умолчанию

Нет

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте данную команду, чтобы создать политику RA Guard Policy и войти в режим RA Guard Policy Configuration Mode.

#### Пример

В данном примере показано, как создать политику RA Guard Policy под именем «policy1».

```
Switch# configure terminal
Switch(config)# ipv6 nd rguard policy policy1
Switch(config-ra-guard)#
```

### 53-2 device-role

Данная команда используется для указания роли подключенного устройства. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
device-role {host | router}
no device-role
```

#### Параметры

<b>host</b>	Укажите, чтобы настроить подключенное устройство в качестве узла (Host).
<b>router</b>	Укажите, чтобы настроить подключенное устройство в качестве маршрутизатора (Router).

#### По умолчанию

Роль по умолчанию – Host.

### Режим ввода команды

RA Guard Policy Configuration Mode

### Использование команды

Используйте данную команду, чтобы указать роль подключенного устройства. Так как по умолчанию устройство выполняет роль узла, получаемые Router Advertisement (RA) и сообщения переадресации будут заблокированы. Если устройство настроено в качестве маршрутизатора, Router Solicitation (RS), Router Advertisement (RA) и сообщения переадресации будут разрешены на данном порту.

### Пример

В данном примере показано, как создать политику RA Guard Policy под именем «raguard1» и настроить устройство в качестве узла.

```
Switch# configure terminal
Switch(config)# ipv6 nd raguard policy raguard1
Switch(config-ra-guard)# device-role host
Switch(config-ra-guard)#
```

## 53-3 match ipv6 access-list

Данная команда используется для фильтрации RA-сообщений на основе IPv6-адреса отправителя. Используйте форму **no**, чтобы отключить фильтрацию.

```
match ipv6 access-list IPV6-ACCESS-LIST-NAME
no match ipv6 access-list
```

### Параметры

---

<i>IPV6-ACCESS-LIST-NAME</i>	Укажите стандартный список доступа IPv6.
------------------------------	--

---

### По умолчанию

Нет

### Режим ввода команды

RA Guard Policy Configuration Mode

### Использование команды

Используйте данную команду для устройства в роли маршрутизатора (Router), чтобы отфильтровать RA-сообщения на основе IP-адреса отправителя. Если команда **match ipv6 access-list** не настроена, все RA-сообщения будут игнорироваться. Список доступа настраивается с помощью команды **ipv6 access-list**.

### Пример

В данном примере показано, как создать политику RA Guard Policy и настроить проверку соответствия IPv6-адресов списку доступа «list1».

```
Switch# configure terminal
Switch(config)# ipv6 nd raguard policy raguard1
Switch(config-ra-guard)# match ipv6 access-list list1
Switch(config-ra-guard)#
```

### 53-4 ipv6 nd raguard attach-policy

Данная команда используется для применения политики RA Guard Policy на определенном интерфейсе. Используйте форму **no**, чтобы удалить привязку.

```
ipv6 nd raguard attach-policy [POLICY-NAME]
no ipv6 nd raguard
```

#### Параметры

<i>POLICY-NAME</i>	(Опционально) Укажите имя политики RA Guard Policy.
--------------------	---

#### По умолчанию

Нет

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

Может быть применена только одна политика RA Policy. Если имя политики не указано, политика по умолчанию настроит устройство в качестве узла.

#### Пример

В данном примере показано, как применить политику RA Guard Policy на интерфейсе Ethernet 1/0/3.

```
Switch# configure terminal
Switch(config)# ipv6 nd raguard policy raguard1
Switch(config-ra-guard)# device-role router
Switch(config-ra-guard)# match ipv6 access-list list1
Switch(config-ra-guard)# exit
Switch(config)# interface eth1/0/3
Switch(config-if)# ipv6 nd raguard attach-policy raguard1
Switch(config-if)#
```

### 63-5 show ipv6 nd raguard policy

Данная команда используется для отображения информации о политике RA Guard Policy.

```
show ipv6 nd raguard policy [POLICY-NAME]
```

## Параметры

---

<i>POLICY-NAME</i>	(Опционально) Укажите имя политики RA Guard Policy.
--------------------	---

---

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Если имя политики указано, отображаться будет информация только для указанной политики. Если имя политики не указано, отображаться будет информация для всех политик.

### Пример

В данном примере показано, как отобразить конфигурацию политики под именем «raguard1» на всех интерфейсах, на которых применена данная политика.

```
Switch# show ipv6 nd raguard policy raguard1

Policy raguard1 configuration:
  Device Role: host
  Target: eth1/0/1-1/0/2

Switch#
```

## 54. Команды Safeguard Engine

### 54-1 clear cpu-protect counters

Данная команда используется для обнуления счетчиков защиты ЦПУ.

**clear cpu-protect counters {all | sub-interface [manage | protocol | route] | type [PROTOCOL-NAME]}**

#### Параметры

<b>all</b>	Укажите для обнуления всех счетчиков защиты ЦПУ.
<b>sub-interface [manage   protocol   route]</b>	Укажите для обнуления счетчиков защиты ЦПУ под-интерфейсов. Если под-интерфейс не указан, будут обнулены счетчики защиты ЦПУ всех под-интерфейсов.
<b>type [PROTOCOL-NAME]</b>	Укажите для обнуления счетчиков защиты ЦПУ определенного протокола. Если имя протокола не указано, будут обнулены счетчики защиты ЦПУ всех протоколов.

#### По умолчанию

Нет

#### Режим ввода команды

Privileged EXEC Mode

#### Использование команды

При вводе команды без параметров будут обнулены все счетчики защиты ЦПУ.

#### Пример

В данном примере показано, как удалить всю статистику защиты ЦПУ.

```
Switch# clear cpu-protect counters all
Switch#
```

### 54-2 cpu-protect safeguard

Данная команда используется для включения или настройки функции Safeguard Engine. Используйте форму **no**, чтобы отключить функцию Safeguard Engine.

**cpu-protect safeguard [threshold RISING-THRESHOLD FALLING-THRESHOLD]**  
**no cpu-protect safeguard [threshold]**

#### Параметры

<b>threshold</b>	(Опционально) Укажите, чтобы настроить пороговые значения загрузки, при которой будет включаться/отключаться функция Safeguard Engine.
------------------	--



<i>RISING-THRESHOLD</i>	(Опционально) Укажите, чтобы установить значение в процентах верхнего порога загрузки ЦПУ, при котором включается функция Safeguard Engine. Если загрузка ЦПУ превысит указанное значение, механизм Safeguard Engine начнет функционировать. Доступный диапазон значений: от 20 до 100.
<i>FALLING-THRESHOLD</i>	(Опционально) Укажите, чтобы установить значение в процентах нижнего порога загрузки ЦПУ, при котором выключается функция Safeguard Engine. Если загрузка ЦПУ снизится до указанного значения, механизм Safeguard Engine перестанет функционировать. Доступный диапазон значений: от 20 до 100.

### По умолчанию

По умолчанию функция Safeguard Engine отключена.  
Верхний порог загрузки ЦПУ по умолчанию – 70.  
Нижний порог загрузки ЦПУ по умолчанию – 20.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Safeguard Engine позволяет сохранить устройство в работоспособном состоянии при атаке, минимизируя рабочую загрузку коммутатора и одновременно давая возможность пересылать важные пакеты по сети в ограниченной полосе пропускания. Если загрузка ЦПУ превышает установленный верхний порог, коммутатор переходит в режим высокой загрузки (Exhausted Mode). В данном режиме коммутатор ограничивает полосу пропускания принимаемых ARP-пакетов и широковещательных IP- пакетов.

### Пример

В данном примере показано, как включить Safeguard Engine и настроить пороговые значения. Верхнее пороговое значение – 60. Нижнее пороговое значение – 40.

```
Switch# configure terminal
Switch(config)# cpu-protect safeguard threshold 60 40
Switch(config)#
```

## 54-3 cpu-protect sub-interface

Данная команда используется для настройки пропускной способности (Rate Limit) трафика, предназначенного для ЦПУ по типам под-интерфейсов. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
cpu-protect sub-interface {manage | protocol | route} pps RATE
no cpu-protect sub-interface {manage | protocol | route}
```

### Параметры

<b>pps RATE</b>	Укажите пороговое значение. Единица измерения – пакеты в секунду. Если установлено значение 0, будут отброшены
-----------------	--

---

все пакеты указанных типов под-интерфейса.

---

**По умолчанию**

Нет

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Причины, по которым пакеты предназначаются для ЦПУ, могут быть классифицированы по следующим трем группам: **manage**, **protocol** и **route**. Под-интерфейс – это логический интерфейс, предназначенный для разделения полученных пакетов ЦПУ на разные группы. Как правило, для корректной работы функций пакеты протокола должны иметь более высокий приоритет. Обычно ЦПУ не участвует в маршрутизации пакетов. В некоторых случаях, например, при изучении нового IP- адреса, или если не указан маршрут по умолчанию, некоторые пакеты будут опрарлены в ЦПУ для программной маршрутизации. Используйте данную команду, чтобы ограничить скорость маршрутизируемых пакетов. Это позволит ЦПУ не тратить много времени на маршрутизацию пакетов.

**Пример**

В данном примере показано, как настроить пропускную способность (Rate Limit) пакетов для под-интерфейса управления (Management). Настроенное пороговое значение – 1000 пакетов в секунду.

```
Switch# configure terminal
Switch(config)# cpu-protect sub-interface manage pps 1000
Switch(config)#
```

**54-4 cpu-protect type**

Данная команда используется для настройки пропускной способности (Rate Limit) трафика, предназначенного для ЦПУ типом протокола. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**cpu-protect type** *PROTOCOL-NAME* **pps** *RATE*  
**no** **cpu-protect type** *PROTOCOL-NAME*

**Параметры**

<i>PROTOCOL-NAME</i>	Укажите имя протокола, который необходимо настроить.
<b>pps</b> <i>RATE</i>	Укажите пороговое значение. Единица измерения – пакеты в секунду. Если установлено значение 0, будут отброшены все пакеты указанного протокола.

**По умолчанию**

Нет

**Режим ввода команды**

Global Configuration Mode

## Уровень команды по умолчанию

Уровень 12

### Использование команды

ЦПУ должно обрабатывать следующие пакеты: протоколы маршрутизации, протоколы 2 уровня и пакеты для управления. ЦПУ, перегруженное предназначенным для него трафиком, будет тратить много времени на обработку ненужного трафика, что повлияет на процессы маршрутизации. Чтобы уменьшить нагрузку на ЦПУ, используйте данную команду для настройки порогового значения пакетов указанного протокола.

В соответствии с назначением пакетов, предназначенных для ЦПУ, маршрутизатор создает три виртуальных под-интерфейса для обработки пакетов:

- **manage** – пакеты предназначены для любого интерфейса маршрутизатора или интерфейса системы управления сетью через протокол интерактивного доступа, такого как Telnet или SSH;
- **protocol** – управляющие пакеты протокола, которые могут быть идентифицированы маршрутизатором;
- **route** – другие пакеты, поступающие на маршрутизатор для маршрутизации, которые должны быть обработаны ЦПУ, прежде чем это будет сделано без участия ЦПУ.

В таблице ниже перечислены имена поддерживаемых протоколов для данной команды:

Имя протокола	Описание	Классификация (sub-интерфейс)
<b>8021x</b>	Port-based Network Access Control	Protocol
<b>arp</b>	IP Address Resolution Protocol (ARP)	Protocol
<b>dhcp</b>	Dynamic Host Configuration	Protocol
<b>dns</b>	Domain Name Services	Protocol
<b>gvrp</b>	GARP VLAN Registration Protocol	Protocol
<b>icmpv4</b>	IPv4 Internet Control Message Protocol	Protocol
<b>icmpv6-neighbor</b>	IPv6 ICMP Neighbor Discover Protocol (NS/NA/RS/RA)	Protocol
<b>icmpv6-other</b>	IPv6 ICMP except NDP NS/NA/RS/RA	Protocol
<b>igmp</b>	Internet Group Management Protocol	Protocol
<b>snmp</b>	Simple Network Management Protocol	Manage
<b>ssh</b>	Secured shell	Manage
<b>stp</b>	Spanning Tree Protocol (802.1D)	Protocol
<b>telnet</b>	Telnet	Manage
<b>tftp</b>	Trivial File Transfer Protocol	Manage
<b>web</b>	HTTP and HTTPS	Manage

### Пример

В данном примере показано, как настроить пороговое значение пакетов протокола OSPF. Настроенное пороговое значение – 100 пакетов в секунду.

```
Switch# configure terminal
Switch(config)# cpu-protect type ospf pps 100
Switch(config)#
```

## 54-5 show cpu-protect safeguard

Данная команда используется для отображения настроек и статуса функции Safeguard Engine.

### show cpu-protect safeguard

#### Параметры

Нет

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте данную команду, чтобы отобразить настройки и статус функции Safeguard Engine.

#### Пример

В данном примере показано, как отобразить настройки и текущий статус Safeguard Engine.

```
Switch#show cpu-protect safeguard

Safeguard Engine State: Disabled
Safeguard Engine Status: Normal
Utilization Thresholds:
  Rising   :50%
  Falling  :20%

Switch#
```

#### Отображаемые параметры

<b>Safeguard Engine Status</b>	Текущий режим загрузки ЦПУ. Возможны следующие строки для отображения: <b>Exhausted:</b> если загрузка ЦПУ превышает установленный верхний порог, коммутатор переходит в режим Exhausted Mode, и механизм Safeguard Engine начинает функционировать. Safeguard Engine не выключается до тех пор, пока загрузка не снизится до нижнего порога. <b>Normal:</b> Safeguard Engine не срабатывает.
--------------------------------	---

## 54-6 show cpu-protect sub-interface

Данная команда используется для отображения пропускной способности (Rate Limit) и статистики под-интерфейса.

### **show cpu-protect sub-interface {manage | protocol | route}**

#### Параметры

<b>manage</b>	Указывает отображаемый суб-интерфейс менеджера.
<b>protocol</b>	Указывает отображаемый подинтерфейс протокола.
<b>route</b>	Указывает отображаемый подинтерфейс маршрута.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте эту команду для отображения настроенного ограничения скорости и количества падений для защитного механизма определенной группы. Эти счетчики подсчитываются программным обеспечением.

#### Пример

В этом примере показано, как отобразить настроенное ограничение скорости и количество падений для защитного механизма определенной группы.

```
Switch#show cpu-protect sub-interface manage
Sub-Interface: manage
Rate Limit: N/A
Switch#
```

## 54-7 show cpu-protect type

Данная команда используется для отображения пропускной способности (Rate Limit) и статистики защиты ЦПУ.

### **show cpu-protect type *PROTOCOL-NAME***

#### Параметры

<b><i>PROTOCOL-NAME</i></b>	Указывает настроенное ограничение скорости и статистику указанного протокола для отображения.
-----------------------------	---

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте данную команду, чтобы отобразить Rate Limit и статистику механизма Safeguard Engine.

#### Пример

В данном примере показано, как отобразить Rate Limit и статистику механизма Safeguard Engine.

```
Switch#show cpu-protect type arp

Type: arp
Rate Limit: N/A

Switch#
```

## 54-8 snmp-server enable traps safeguard-engine

Данная команда используется для включения отправки SNMP-уведомлений для Safeguard Engine. Используйте форму **no**, чтобы отключить отработку SNMP-уведомлений для Safeguard Engine.

**snmp-server enable traps safeguard-engine**  
**no snmp-server enable traps safeguard-engine**

#### Параметры

Нет

#### По умолчанию

По умолчанию данная функция отключена.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте данную команду, чтобы включить/отключить отработку SNMP-уведомлений при изменении текущего режима Safeguard Engine.

#### Пример

В данном примере показано, как включить отработку trap-сообщений об изменении текущего режима Safeguard Engine.

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

## 55. Команды Secure Shell (SSH)

### 55-1 crypto key generate

Данная команда используется для генерирования пары ключей RSA или DSA.

**crypto key generate {rsa [modulus *MODULUS-SIZE*] | dsa}**

#### Параметры

<b>rsa</b>	Укажите для генерирования пары ключей RSA.
<b>modulus <i>MODULUS-SIZE</i></b>	(Опционально) Укажите количество битов в модуле. Доступные значения для RSA: 360, 512, 768, 1024 и 2048. Если не указано, будет получено сообщение о необходимости указать значение.
<b>dsa</b>	Укажите для генерирования пары ключей DSA. Фиксированный размер ключа DSA – 1024 битов.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Данная команда используется для генерирования пары ключей RSA или DSA.

#### Пример

В данном примере показано, как создать ключ RSA.

```
Switch# crypto key generate rsa

The RSA key pairs already existed.
Do you really want to replace them? (y/n) [n]y
Choose the size of the key modulus in the range of 360 to 2048.The process may take
a few minutes.
Number of bits in the modulus [768]: 768
Generating RSA key...Done

Switch#
```

### 55-2 crypto key zeroize

Данная команда используется для удаления пары ключей RSA или DSA.

**crypto key zeroize {rsa | dsa}**



**Параметры**

<b>rsa</b>	Укажите, чтобы удалить пару ключей RSA.
<b>dsa</b>	Укажите, чтобы удалить пару ключей DSA.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте данную команду, чтобы удалить пару открытых ключей SSH-сервера. Если обе пары ключей RSA и DSA удалены, SSH-сервер будет недоступен.

**Пример**

В данном примере показано, как удалить ключ RSA.

```
Switch# crypto key zeroize rsa
Do you really want to remove the key? (y/n)[n]: y
Switch#
```

**55-3 ip ssh timeout**

Данная команда используется для настройки параметров контроля SSH на коммутаторе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip ssh {timeout SECONDS | authentication-retries NUMBER}
no ip ssh {timeout | authentication-retries}
```

**Параметры**

<b>timeout SECONDS</b>	Укажите временной интервал ожидания ответа от SSH-клиента для этапа согласования SSH. Доступный диапазон значений: от 30 до 600.
<b>authentication-retries NUMBER</b>	Укажите количество попыток аутентификации. Сессия завершается после всех неудачных попыток. Доступный диапазон значений: от 1 до 32.

**По умолчанию**

По умолчанию значение тайм-аута – 120 секунд.

По умолчанию количество попыток аутентификации – 3.

**Режим ввода команды**

Global Configuration Mode

### Использование команды

Используйте данную команду, чтобы настроить параметры SSH-сервера на коммутаторе. С помощью параметра **authentication-retries** укажите максимальное количество попыток аутентификации перед завершением сессии.

### Пример

В данном примере показано, как настроить значение тайм-аута SSH на 160 секунд.

```
Switch# configure terminal
Switch(config)# ip ssh timeout 160
Switch(config)#
```

В данном примере показано, как настроить значение попыток аутентификации. Настроенное значение – 2. Соединение будет прервано после 2 неудачных попыток.

```
Switch# configure terminal
Switch(config)# ip ssh authentication-retries 2
Switch(config)#
```

## 55-4 ip ssh server

Данная команда используется для включения SSH-сервера. Используйте форму **no**, чтобы отключить SSH-сервер.

```
ip ssh server
no ip ssh server
```

### Параметры

Нет

### По умолчанию

По умолчанию SSH-сервер отключен.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду, чтобы включить SSH-сервер.

### Пример

В данном примере показано, как включить SSH-сервер.

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

## 55-5 ip ssh service-port

Данная команда используется для указания сервисного порта для SSH. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip ssh service-port TCP-PORT
no ip ssh service-port
```

### Параметры

<i>TCP-PORT</i>	Укажите номер TCP-порта. Доступный диапазон значений: от 1 до 65535. Как правило, для протокола SSH назначается TCP-порт 22.
-----------------	---

### По умолчанию

По умолчанию номер TCP-порта – 22.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду, чтобы настроить номер TCP-порта для SSH-сервера.

### Пример

В данном примере показано, как изменить номер сервисного порта. Новый настроенный номер – 3000.

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

## 55-6 show crypto key mypubkey

Данная команда используется для отображения пар открытых ключей RSA или DSA.

```
show crypto key mypubkey {rsa | dsa}
```

### Параметры

<b>rsa</b>	Укажите, чтобы отобразить информацию об открытом ключе RSA.
<b>dsa</b>	Укажите, чтобы отобразить информацию об открытом ключе DSA.

### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте данную команду, чтобы отобразить пары открытых ключей RSA или DSA.

#### Пример

В данном примере показано, как отобразить информацию об открытом ключе RSA.

```
Switch# show crypto key mypubkey rsa

% Key pair was generated at: 09:48:40, 2013-11-29
Key Size: 768 bits
Key Data:
AAAAB3Nz aC1yc2EA AAADAQAB AAAAQwCN 6IRFHCBF jsHvYjQG iCL0p2kz 2v38ULC8
kAKra/Ze mG7IW3eC 8STcrkr5 s719H/bh jG/oqkwj S1UJSGqR e/sj6Ns=

Switch#
```

## 55-7 show ip ssh

Данная команда используется для отображения пользовательских настроек конфигурации SSH.

### show ip ssh

#### Параметры

Нет

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте данную команду, чтобы отобразить настройки конфигурации SSH.

#### Пример

В данном примере показано, как отобразить настройки конфигурации SSH.

```
Switch# show ip ssh

IP SSH server      : Enabled
IP SSH service port : 22
SSH server mode    : V2
Authentication timeout : 120 secs
Authentication retries : 3 times

Switch#
```

## 55-8 show ssh

Данная команда используется для отображения статуса подключений SSH-сервера.

**show ssh**

### Параметры

Нет

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте данную команду, чтобы отобразить статус подключений SSH на коммутаторе.

### Пример

В данном примере показано, как отобразить информацию о подключениях SSH.

```
Switch# show ssh

SID Ver. Cipher                               Userid           Client IP Address
-----
0  V2  3des-cbc/sha1-96                            zhang3           192.168.0.100
1  V2  3des-cbc/hmac-sha1                          lee4567890123456 2000::243

Total Entries: 2

Switch#
```

### Отображаемые параметры

<b>SID</b>	Уникальный номер, идентифицирующий сессию SSH.
<b>Ver</b>	Версия SSH указанной сессии.
<b>Cipher</b>	Криптографический/Hashed Message Authentication Code

	(HMAC) алгоритм, используемый SSH-клиентом.
<b>Userid</b>	Имя пользователя сессии.
<b>Client IP Address</b>	IP-адрес клиента для установленной сессии SSH.

## 55-9 ssh user authentication-method

Данная команда используется для настройки методов аутентификации SSH для учетной записи пользователя. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ssh user NAME authentication-method {password | publickey URL | hostbased URL host-name
HOSTNAME [IP-ADDRESS | IPV6-ADDRESS]}
no ssh user NAME authentication-method
```

### Параметры

<i>NAME</i>	Укажите имя пользователя для настройки типа аутентификации. Имя пользователя должно быть существующей локальной учетной записью. Максимально допустимое количество символов – 32.
<b>password</b>	Укажите метод аутентификации по паролю для указанной учетной записи пользователя. Данный метод аутентификации используется по умолчанию.
<b>publickey URL</b>	Укажите метод аутентификации с открытым ключом для указанной учетной записи пользователя. Введите URL локального файла, который будет использоваться в качестве открытого ключа указанного пользователя.
<b>hostbased URL</b>	Укажите метод аутентификации на основе узла для указанной учетной записи пользователя. Введите URL локального файла, который будет использоваться в качестве ключа узла клиента.
<b>host-name HOSTNAME</b>	Укажите доступное имя узла для аутентификации на основе узла. Имя узла клиента проверяется во время аутентификации. Доступный диапазон значений: от 1 до 255.
<i>IP-ADDRESS</i>	(Опционально) Укажите необходима ли дополнительная проверка IP- адреса клиента для аутентификации на основе узла. Если не указано, будет проверено только имя узла.
<i>IPV6-ADDRESS</i>	(Опционально) Укажите необходима ли дополнительная проверка IPv6- адреса клиента для аутентификации на основе узла. Если не указано, будет проверено только имя узла.

### По умолчанию

По умолчанию используется метод аутентификации по паролю.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду, чтобы настроить метод аутентификации для пользователя. Имя пользователя должно быть пользователем, созданным при помощи команды **username**. По умолчанию используется метод аутентификации по паролю. Системой будет предложено ввести пароль.

Для аутентификации пользователя при помощи открытого ключа SSH скопируйте файл открытого ключа пользователя в файловую систему. Когда пользователь пытается войти в учетную запись на коммутаторе через SSH-клиента (используя метод открытого ключа SSH), SSH-клиент автоматически передаст коммутатору открытый ключ и подпись с закрытым ключом. Если и открытый ключ, и подпись верны, пользователь будет аутентифицирован, и вход в учетную запись коммутатора будет разрешен.

- Для аутентификации пользователя при помощи открытого ключа SSH или метода на основе узла необходимо указать файл открытого ключа пользователя или файл ключа узла клиента в одном и том же формате. Файл ключа может содержать несколько ключей. Каждый ключ должен быть определен одной строкой. Максимально допустимая длина строки составляет 8 Кб.
- Каждый ключ состоит из следующих разделенных пробелами полей: *keytype*, *base64-encoded key*, *comment*. Ввод полей *keytype* и *base64-encoded key* обязателен, ввод поля *comment* – необязателен. Поле *keytype* может являться *ssh-dss* или *ssh-rsa*.

### Пример

В данном примере показано, как настроить метод аутентификации с открытым ключом для пользователя «user1».

```
Switch# configure terminal
Switch(config)# ssh user user1 authentication-method publickey c:/user1.pub
Switch(config)#
```

## 56. Команды уровня Secure Sockets Layer (SSL)

### 56-1 no certificate

Данная команда используется для удаления импортированного сертификата.

**no certificate** *NAME*

#### Параметры

<i>NAME</i>	Укажите имя сертификата, который необходимо удалить.
-------------	--

#### По умолчанию

Нет

#### Режим ввода команды

Certificate Chain Configuration Mode

#### Использование команды

Используйте команду **show crypto pki trustpoints**, чтобы отобразить список имен импортированных сертификатов. Затем в команде **no certificate** укажите импортированные сертификаты доверенной точки (Trust Point), которые необходимо удалить. Если указанный сертификат является локальным, соответствующий закрытый ключ также будет удален.

#### Пример

В данном примере показано, как удалить импортированный сертификат. Имя сертификата – tongken.ca. Trust Point – gaa.

```
Switch# show crypto pki trustpoints

Trustpoint Name      : gaa (primary)
  Imported certificates:
    CA                : tongken.ca
    local certificate  : webserver.crt
    local private key  : webserver.prv

Switch# configure terminal
Switch(config)# crypto pki certificate chain gaa
Switch(config-cert-chain)# no certificate tongken.ca
Switch(config-cert-chain)#
```

### 56-2 crypto pki import pem



Данная команда используется для импорта сертификата ЦС (Центра Сертификации/Certificate Authority) или сертификата коммутатора и ключей в Trust Point из файлов в формате PEM (Privacy- Enhanced Mail).

```
crypto pki import TRUSTPOINT pem FILE-SYSTEM:[DIRECTORY/]FILE-NAME [password PASSWORD-PHRASE] {ca | local | both}
```

```
crypto pki import TRUSTPOINT pem tftp://IP-ADDRESS/ [DIRECTORY/]FILE-NAME [password PASSWORD-PHRASE] {ca | local | both}
```

### Параметры

<i>TRUSTPOINT</i>	Укажите имя Trust Point, которое ассоциировано с импортированными сертификатами и парами ключей.
<i>FILE-SYSTEM</i>	Укажите файловую систему для сертификатов и пар ключей. После указанной файловой системы необходимо использовать двоеточие «:».
<i>DIRECTORY</i>	(Опционально) Укажите имя каталога для импорта сертификатов и пар ключей. Возможен импорт в коммутатор или на TFTP-сервер.
<i>FILE-NAME</i>	Укажите имя сертификатов и пар ключей, которые необходимо импортировать. По умолчанию к имени сертификата ЦС добавляется .ca, к закрытому ключу – .prv и к сертификату – .crt.
<b>password</b> <i>PASSWORD-PHRASE</i>	(Опционально) Укажите зашифрованную фразу пароля для отмены шифрования при импорте закрытых ключей. Максимально допустимое количество символов в строке – 64. Если фраза пароля не указана, используется пустая строка.
<b>tftp</b>	Укажите URL источника для сетевого TFTP-сервера.
<i>IP-ADDRESS</i>	Укажите IP-адрес TFTP-сервера.
<b>ca</b>	Укажите, чтобы импортировать только сертификат ЦС.
<b>local</b>	Укажите, чтобы импортировать локальный сертификат и пары ключей.
<b>both</b>	Укажите, чтобы импортировать сертификат ЦС, локальный сертификат и пары ключей.

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

Данная команда позволяет администраторам импортировать сертификаты и пары ключей в файлы в формате PEM.

Соответствующие сертификаты и пары ключей необходимо импортировать в коммутатор в соответствии с желаемым алгоритмом обмена ключами. Сертификаты/пары ключей RSA и DSA должны быть импортированы для RSA и DHS-DSS соответственно. Сертификаты и ключи RSA и DSA несовместимы. SSL-

клиент, имеющий только сертификат и ключ RSA, не может установить соединение с SSL-сервером, у которого есть только сертификат и ключ DSA.

Импортированные сертификат(ы) могут образовывать цепочку, которая устанавливает последовательность доверенных сертификатов: от сертификата узла до корневого сертификата ЦС. Точка доверия ЦС (Trust Point CA) – это центр сертификации (Certificate Authority, CA), настроенный на коммутаторе в качестве доверенного ЦС. Любой полученный сертификат узла будет принят, если он подтвержден локальным доверенным ЦС или его подчиненными.

Если указанной доверенной точки не существует, появится сообщение об ошибке.

### Пример

В данном примере показано, как импортировать файлы сертификатов (ЦС и локальных) и пары ключей в Trust Point «TP1» через TFTP.

```
Switch# configure terminal
Switch(config)# crypto pki import TP1 pem tftp: //10.1.1.2/name/msca password abcd1234 both

% Importing CA certificate...
Destination filename [name/msca.ca]?
Reading file from tftp://10.1.1.2/name/msca.ca
Loading name/msca.ca from 10.1.1.2 (via eth1/0/5):!
[OK - 1082 bytes]

% Importing private key PEM file...
Reading file from tftp://10.1.1.2/name/msca.prv
Loading name/msca.prv from 10.1.1.2 (via eth1/0/5):!
[OK - 573 bytes]

% Importing certificate PEM file...
Reading file from tftp://10.1.1.2/name/msca.crt
Loading name/msca.crt from 10.1.1.2 (via eth1/0/5):!
[OK - 1289 bytes]
% PEM files import succeeded.

Switch(config)#
```

## 56-3 crypto pki trustpoint

Данная команда используется для настройки Trust Point, которую будет использовать коммутатор. Используйте форму **no**, чтобы удалить все сертификаты и пары ключей, ассоциированные с признанной Trust Point.

```
crypto pki trustpoint NAME
no crypto pki trustpoint NAME
```

### Параметры

---

*NAME*

Укажите для создания имени Trust Point.

---

**По умолчанию**

Нет

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Используйте эту команду для объявления точки доверия, которая может быть самоподписанным корневым центром сертификации (CA) или подчиненным CA. При вводе этой команды вы войдете в режим конфигурации CA-Trust-Point.

**Пример**

В данном примере показано, как настроить Trust Point «TP1» и указать ее в качестве основной.

```
Switch# configure terminal
Switch(config)# crypto pki trustpoint TP1
Switch(ca-trustpoint)# primary
Switch(ca-trustpoint)#
```

**56-4 crypto pki certificate chain**

Данная команда используется для входа в режим конфигурации Certificate Chain Configuration Mode.

**crypto pki certificate chain** *NAME*

**Параметры**

<i>NAME</i>	Укажите имя Trust Point.
-------------	--------------------------

**По умолчанию**

Нет

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Используйте данную команду, чтобы войти в режим конфигурации Certificate Chain Configuration Mode. Если указанного имени Trust Point не существует, будет отображено сообщение об ошибке.

**Пример**

В данном примере показано, как войти в режим конфигурации Certificate Chain Configuration Mode.

```
Switch# configure terminal
Switch(config)# crypto pki certificate chain TP1
Switch(trustpoint)#
```

## 56-5 primary

Данная команда используется для назначения указанной Trust Point в качестве основной Trust Point коммутатора. Используйте форму **no**, чтобы отменить назначение.

**primary**  
**no primary**

### Параметры

Нет

### По умолчанию

По умолчанию данная функция отключена.

### Режим ввода команды

CA-Trust-Point Configuration Mode

### Использование команды

Используйте данную команду, чтобы указать Trust Point в качестве основной. Указанная Trust Point будет использоваться по умолчанию, если система не может определить, какую Trust Point центра сертификации необходимо использовать. В качестве основной может быть указана только одна Trust Point. После указания Trust Point в качестве основной, предыдущая Trust Point будет перезаписана.

### Пример

В данном примере показано, как настроить Trust Point «TP1» в качестве основной.

```
Switch# configure terminal
Switch(config)# crypto pki trustpoint TP1
Switch(ca-trustpoint)# primary
Switch(ca-trustpoint)#
```

## 56-6 show crypto pki trustpoints

Данная команда используется для отображения Trust Point, настроенных на коммутаторе.

**show crypto pki trustpoints** [*TRUSTPOINT*]

### Параметры

---

*TRUSTPOINT*

(Опционально) Укажите имя Trust Point, которую необходимо отобразить.

---

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Если параметры не указаны, отобразятся все Trust Point.

### Пример

В данном примере показано, как отобразить все Trust Point.

```
Switch# show crypto pki trustpoints

Trustpoint Name      : TP1 (primary)
  Imported certificates:
    CA                : tongken.ca
    local certificate  : webservr.crt
    local private key  : webservr.prv

Trustpoint Name      : TP2
  Imported certificates:
    CA                : chunagtel.ca
    local certificate  : openflow.crt
    local private key  : openflow.prv

Switch#
```

## 56-7 show ssl-service-policy

Данная команда используется для отображения политики SSL Service Policy.

**show ssl-service-policy** [*POLICY-NAME*]

### Параметры

<i>POLICY-NAME</i>	(Опционально) Укажите имя политики SSL Service Policy.
--------------------	--

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Если имя политики SSL Service Policy не указано, отобразятся все SSL Service Policy.

### Пример

В данном примере показано, как отобразить все SSL Service Policy.

```

Switch# show ssl-service-policy

SSL Policy Name      : policyForHttp
  Enabled Versions  :
    TLS 1.0
    TLS 1.1
    TLS 1.2
  Enabled CipherSuites :
    DHE_DSS_WITH_3DES_EDE_CBC_SHA,
    RSA_WITH_3DES_EDE_CBC_SHA,
    RSA_WITH_RC4_128_SHA,
    RSA_WITH_RC4_128_MD5,
    RSA_EXPORT_WITH_RC4_40_MD5
    RSA_WITH_AES_128_CBC_SHA
    RSA_WITH_AES_256_CBC_SHA
    RSA_WITH_AES_128_CBC_SHA256
    RSA_WITH_AES_256_CBC_SHA256
    DHE_DSS_WITH_AES_256_CBC_SHA
    DHE_RSA_WITH_AES_256_CBC_SHA
  Session Cache Timeout: 600
  Secure Trustpoint   : ggg

SSL Policy Name      : policyForFTP
  Enabled Versions  :
    TLS 1.0
    TLS 1.1
    TLS 1.2
  Enabled CipherSuites :
    RSA_WITH_RC4_128_MD5,
    RSA_EXPORT_WITH_RC4_40_MD5
  Session Cache Timeout: 1200
  Secure Trustpoint   : domain2

Switch#

```

## 56-8 ssl-service-policy

Данная команда используется для настройки политики SSL Service Policy.

**ssl-service-policy POLICY-NAME** [version [VERSION] | ciphersuite [CIPHERSUITE] | secure-trustpoint TRUSTPOINT | session-cache-timeout TIME-OUT]

**no ssl-service-policy POLICY-NAME** [version [VERSION] | ciphersuite [CIPHERSUITE] | secure-trustpoint TRUSTPOINT | session-cache-timeout TIME-OUT]

## Параметры

<i>POLICY-NAME</i>	Укажите имя политики SSL Service Policy.
<b>version</b> <i>VERSION</i>	(Опционально) Указывает версию TLS. Можно использовать одно из следующих ключевых слов: <b>tls1.0</b> – Указывает на использование TLS версии 1.0 в качестве политики службы SSL. <b>tls1.1</b> – Указывает на использование TLS версии 1.1 в качестве политики службы SSL.
<b>ciphersuite</b>	(Опционально) Укажите шифрование Cipher Suite, которое будет использоваться служба безопасности при установлении соединения с удаленным узлом. Используйте обмен ключами DH с шифрованием 3DES-EDE-CBC и SHA для дайджеста сообщений – <b>dhe-dss-3des-ede-cbc-sha</b> . Используйте обмен ключами RSA с шифрованием 3DES и DES-EDE3- CBC и Secure Hash Algorithm (SHA) для дайджеста сообщений – <b>rsa-3des-ede-cbc-sha</b> . Используйте обмен ключами RSA с 128-битным шифрованием RS4 и SHA для дайджеста сообщений – <b>rsa-rc4-128-sha</b> . Используйте обмен ключами RSA с 128-битным шифрованием RS4 и Message Digest 5 (MD5) для дайджеста сообщений – <b>rsa-rc4-128-md5</b> . Используйте обмен ключами RSA EXPORT с 40-битным шифрованием RS4 и MD5 для дайджеста сообщений – <b>rsa-export-rc4-40-md5</b> . Если шифрование Cipher Suite не настроено, клиент и сервер SSL согласовывают наиболее подходящее шифрование из списка доступных Cipher Suite. Будет выбрано шифрование, которое поддерживается и SSL-клиентом, и SSL-сервером. Возможно использование нескольких Cipher Suite. Используйте форму <b>no</b> , чтобы отключить выбранные Cipher Suite.
<b>secure-trustpoint</b> <i>TRUSTPOINT</i>	(Опционально) Укажите имя Trust Point, которую необходимо использовать при установке SSL. Если данный параметр не указан, будет использоваться Trust Point, выступающая в роли основной. Если основная Trust Point не указана, будет использоваться встроенный сертификат/пары ключей. Используйте форму <b>no</b> , чтобы отменить указанные Trust Point и использовать встроенный сертификат/пары ключей.
<b>session-cache-timeout</b> <i>TIME-OUT</i>	(Опционально) Укажите значение тайм-аута в секундах для информации, хранящейся в кэше SSL-сессий. Доступный диапазон значений: от 60 до 86400. Если данный параметр не настроен, тайм-аут кэша сессий по умолчанию составляет 600 секунд. Используйте форму <b>no</b> , чтобы вернуть настройки по умолчанию для тайм-аута кэша SSL-сессий.

## По умолчанию

Нет

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте данную команду, чтобы настроить политику SSL Service Policy.

#### Пример

В данном примере показано, как настроить политику SSL Service Policy, которая ассоциирована с Trust Point «TP1». Настроенная политика SSL Service Policy – «ssl-server».

```
Switch# configure terminal
Switch(config)# ssl-service-policy ssl-server secure-trustpoint TP1
Switch(config)#
```

## 56-9 crypto pki certificate generate

Эта команда используется для генерации нового self-signed сертификата.

### crypto pki certificate generate

#### Параметры

Нет

#### По умолчанию

По умолчанию коммутатор автоматически генерирует случайный встроенный сертификат.

#### Режим вводакоманды

Global Configuration Mode

#### Использование команды

Используйте эту команду для генерации нового самоподписного сертификата независимо от наличия или отсутствия встроенного самоподписного сертификата. Коммутатор сгенерирует новый самоподписанный сертификат автоматически, если после загрузки коммутатора сертификат не был обнаружен. Сертификат, созданный этой командой, не влияет на загруженные пользователем сертификаты.



**Примечание:** Эта команда поддерживает только самоподписанный RSA-сертификат с длиной ключа 2048.

#### Пример

В этом примере показано, как сгенерировать новый self-signed сертификат.



```
Switch# configure terminal
Switch(config)# crypto pki certificate generate

Start generating key ...
Start generating self-signed certificate ...
Done.
Switch(config)#
```

## 57. Команды протокола Simple Network Management Protocol (SNMP)

### 57-1 show snmp trap link-status

Данная команда используется для отображения состояния trap-статуса состояния линии связи (link- status) на интерфейсе.

```
show snmp trap link-status [interface INTERFACE-ID [, | -]]
```

#### Параметры

<b>interface</b> <i>INTERFACE-ID</i>	(Опционально) Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Данная команда используется для отображения состояния trap-статуса при обнаружении/разрыве соединения состояния link-up/link-down на интерфейсе.

#### Пример

В данном примере показано, как отобразить trap-статус состояния link-up/link-down для диапазона интерфейсов от Ethernet 1/0/1 до Ethernet 1/0/9.

```
Switch# show snmp trap link-status interface eth1/0/1-9
```

Interface	Trap state
eth1/0/1	Enabled
eth1/0/2	Enabled
eth1/0/3	Disabled
eth1/0/4	Enabled
eth1/0/5	Enabled
eth1/0/6	Disabled
eth1/0/7	Enabled
eth1/0/8	Enabled
eth1/0/9	Enabled

```
Switch#
```

## 57-2 show snmp-server

Данная команда используется для отображения глобальных настроек о состоянии SNMP-сервера и настроек, касающихся состояния trap.

**show snmp-server [traps]**

### Параметры

<b>traps</b>	(Опционально) Укажите для отображения настроек, касающихся состояния trap.
--------------	--

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Для отображения глобальных настроек о состоянии SNMP-сервера используйте команду **show snmp-server**.

Для отображения настроек, касающихся состояния trap, используйте команду **show snmp-server traps**.

### Пример

В данном примере показано, как отобразить настройки SNMP-сервера.

```
Switch# show snmp-server

SNMP Server   : Enabled
Name          : SiteA-Switch
Location      : HQ 15F
Contact       : MIS Department II
SNMP UDP Port: 50000
SNMP Response Broadcast Request: Enabled

Switch#
```

В данном примере показано, как отобразить настройки, касающиеся состояния trap.

```
Switch# show snmp-server traps

Global Trap State : Enabled
Individual Trap State:
  Authentication      : Enabled
  linkup              : Enabled
  linkdown            : Enabled
  coldstart           : Enabled
  warmstart           : Disabled

Switch#
```

### 57-3 show snmp-server trap-sending

Данная команда используется для отображения состояния отправки SNMP trap на порту.

**show snmp-server trap-sending [interface *INTERFACE-ID* [, | -]]**

#### Параметры

<i>INTERFACE-ID</i>	(Опционально) Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

**Использование команды**

Используйте данную команду, чтобы отобразить состояние отправки SNMP trap на порту. Если ни один из опциональных параметров не указан, будут отображены все порты.

**Пример**

В данном примере показано, как отобразить состояние отправки SNMP trap для диапазона интерфейсов от Ethernet 1/0/1 до Ethernet 1/0/9.

```
Switch# show snmp-server trap-sending interface eth1/0/1-9
```

Port	Trap Sending
eth1/0/1	Enabled
eth1/0/2	Enabled
eth1/0/3	Disabled
eth1/0/4	Enabled
eth1/0/5	Enabled
eth1/0/6	Disabled
eth1/0/7	Enabled
eth1/0/8	Enabled
eth1/0/9	Enabled

```
Switch#
```

**57-4 snmp-server**

Данная команда используется для включения агента SNMP. Используйте форму **no**, чтобы выключить агента SNMP.

```
snmp-server
no snmp-server
```

**Параметры**

Нет

**По умолчанию**

По умолчанию данная функция отключена.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Менеджер SNMP управляет агентом SNMP: отправляет SNMP-запросы агенту и получает ответы и SNMP-уведомления от агента. Для управления агентом необходимо включить на нем SNMP-сервер.

### Пример

В данном примере показано, как включить SNMP-сервер.

```
Switch# configure terminal
Switch(config)# snmp-server
Switch(config)#
```

## 57-5 snmp-server contact

Данная команда используется для настройки системной контактной информации для устройства. Используйте форму **no**, чтобы удалить настройки.

**snmp-server contact** *TEXT*  
**no snmp-server contact**

### Параметры

<i>TEXT</i>	(Опционально) Укажите системную контактную информацию. Максимально допустимое количество символов в строке – 255. Пробелы в строке допустимы.
-------------	--

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду, чтобы настроить системную контактную информацию для управления устройством.

### Пример

В данном примере показано, как указать строку с системной контактной информацией. Указанная строка – MIS Department II.

```
Switch# configure terminal
Switch(config)# snmp-server contact MIS Department II
Switch(config)#
```

## 57-6 snmp-server enable traps

Данная команда используется для глобального включения отправки SNMP trap. Используйте форму **no**, чтобы отключить отправку SNMP trap.

**snmp-server enable traps**  
**no snmp-server enable traps**

#### Параметры

Нет

#### По умолчанию

По умолчанию данная функция отключена.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте данную команду, чтобы включить отправку SNMP trap глобально на устройстве.

#### Пример

В данном примере показано, как включить отправку SNMP trap глобально.

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

## 57-7 snmp-server enable traps snmp

Данная команда используется для включения отправки всех или определенных SNMP-уведомлений. Используйте форму **no**, чтобы отключить отправку всех или определенных SNMP-уведомлений.

**snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]**  
**no snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]**

#### Параметры

<b>authentication</b>	(Опционально) Укажите для отправки SNMP trap об ошибке аутентификации. Trap-сообщение «authenticationFailuretrap» генерируется, если устройство получает SNMP-сообщение, которое не аутентифицировано должным образом. Метод аутентификации зависит от используемой версии SNMP. При использовании SNMPv1 или SNMPv2с ошибка аутентификации возникает, если пакеты были сформированы с указанием неверной строки Community String. При использовании SNMPv3 ошибка аутентификации возникает, если пакеты были сформированы с указанием неверного ключа аутентификации SHA/MD5.
<b>linkup</b>	(Опционально) Укажите для отправки SNMP-уведомлений об установленном соединении. Trap-сообщение «linkUp (3)» генерируется, если на устройстве установлено соединение хотя бы с одним из каналов связи.

<b>linkdown</b>	(Опционально) Укажите для отправки SNMP-уведомлений о прерванном соединении. Trap-сообщение «linkDown (2)» генерируется, если на устройстве прервано соединение хотя бы с одним из каналов связи.
<b>coldstart</b>	(Опционально) Укажите для отправки SNMP-уведомлений о «холодном» старте.
<b>warmstart</b>	(Опционально) Укажите для отправки SNMP-уведомлений о «горячем» старте.

### По умолчанию

По умолчанию данная функция отключена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду для управления отправкой стандартных SNMP trap. Чтобы включить отправку SNMP-trap, необходимо также включить этот параметр глобально.

### Пример

В данном примере показано, как включить отправку всех SNMP trap на узел 10.9.18.100, используя строку сообщества «public».

```
Switch# configure terminal
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server enable traps snmp
Switch(config)# snmp-server host 10.9.18.100 version 2c public
Switch(config)#
```

В данном примере показано, как включить SNMP trap об ошибке аутентификации.

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

## 57-8 snmp-server location

Данная команда используется для указания информации о системном местоположении. Используйте форму **no**, чтобы удалить настройки.

**snmp-server location TEXT**  
**no snmp-server location**

### Параметры

<i>TEXT</i>	Укажите системное местоположение. Максимально допустимое количество символов в строке – 255. Пробелы в строке допустимы.
-------------	--



**По умолчанию**

Нет

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Используйте данную команду для указания информации о системном местоположении на коммутаторе.

**Пример**

В данном примере показано, как указать строку с информацией о системном местоположении. Указанная строка – HQ 15F.

```
Switch# configure terminal
Switch(config)# snmp-server location HQ 15F
Switch(config)#
```

**57-9 snmp-server name**

Данная команда используется для указания информации о системном имени. Используйте форму **no**, чтобы удалить настройки.

**snmp-server name** *NAME*  
**no snmp-server name**

**Параметры**

<i>NAME</i>	Укажите имя сервера. Максимально допустимое количество символов в строке – 255. Оптимальное количество символов в строке – не более 10.
-------------	---

**По умолчанию**

Имя по умолчанию – Switch.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Используйте данную команду для указания информации о системном имени коммутатора.

**Пример**

В данном примере показано, как настроить системное имя. Настроенное имя – SiteA-switch.

```
Switch# configure terminal
Switch(config)# snmp-server name SiteA-switch
Switch(config)#
```

## 57-10 snmp-server trap-sending disable

Данная команда используется для отключения отправки SNMP trap на порту. Используйте форму **no**, чтобы включить от отправку SNMP trap на порту.

```
snmp-server trap-sending disable
no snmp-server trap-sending disable
```

### Параметры

Нет

### По умолчанию

По умолчанию данная функция включена.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Используйте данную команду для отключения отправки сгенерированных системой SNMP trap с определенного порта. Данная команда не применима для SNMP trap, сгенерированных другой системой и переадресованных на порт.

### Пример

В данном примере показано, как отключить от отправку SNMP trap с интерфейса Ethernet 1/0/8.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/8
Switch(config-if)# snmp-server trap-sending disable
Switch(config-if)#
```

## 57-11 snmp-server service-port

Данная команда используется для настройки номера UDP-порта SNMP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
snmp-server service-port PORT-NUMBER
no snmp-server service-port
```

### Параметры

<i>PORT-NUMBER</i>	Укажите номер UDP-порта. Доступный диапазон значение: от 1 до 65535. Некоторые номера могут конфликтовать с другими протоколами.
--------------------	--

### По умолчанию

Номер по умолчанию – 161.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду для настройки номера UDP-порта SNMP на коммутаторе. Агент будет прослушивать пакеты SNMP Request на сервисном UDP-порту настроенного номера.

### Пример

В данном примере показано, как настроить номер UDP-порта SNMP.

```
Switch# configure terminal
Switch(config)# snmp-server service-port 50000
Switch(config)#
```

## 57-12 snmp-server response broadcast-request

Используйте данную команду, чтобы разрешить серверу отвечать на широковещательные пакеты SNMP GetRequest. Используйте форму **no**, чтобы запретить серверу отвечать на широковещательные пакеты SNMP GetRequest.

**snmp-server response broadcast-request**  
**no snmp-server response broadcast-request**

### Параметры

Нет

### По умолчанию

По умолчанию данная функция отключена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду, чтобы разрешить серверу отвечать на широковещательные пакеты SNMP GetRequest, которые будут отправлены средствами NMS для определения сетевого устройства. Для применения данной функции необходимо включить ответ на широковещательные пакеты GetRequest.

### Пример

В данном примере показано, как разрешить серверу отвечать на широковещательные пакеты SNMP Get Request.

```
Switch# configure terminal
Switch(config)# snmp-server response broadcast-request
Switch(config)#
```

## 57-13 snmp trap link-status

Данная команда используется для включения отправки уведомлений об обнаружении/разрыве соединения (link-up/link-down), произошедшего на интерфейсе. Используйте форму **no**, чтобы отключить отправку.

```
snmp trap link-status
no snmp trap link-status
```

### Параметры

Нет

### По умолчанию

По умолчанию данная функция включена.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Данная команда используется для включения или отключения отправки SNMP trap об обнаружении/разрыве соединения (link-up/link-down) на интерфейсе.

### Пример

В данном примере показано, как отключить отправку SNMP trap об обнаружении/разрыве соединения (link-up/link-down) на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# no snmp trap link-status
Switch(config-if)#
```

## 57-14 show snmp

Данная команда используется для отображения настроек SNMP.

```
show snmp {community | host | view | group | engineID}
```

### Параметры

<b>community</b>	Укажите, чтобы отобразить информацию об SNMP-сообществе.
<b>host</b>	Укажите, чтобы отобразить информацию о получателе SNMP trap.
<b>view</b>	Укажите, чтобы отобразить информацию об SNMP View.
<b>group</b>	Укажите, чтобы отобразить информацию об SNMP-группе.
<b>engineID</b>	Укажите, чтобы отобразить информацию о SNMP local engine ID.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте данную команду для отображения информации об SNMP. При отображении строк SNMP Community String созданные SNMPv1 или SNMPv2c-пользователи не будут отображены.

### Пример

В данном примере показано, как отобразить информацию об SNMP-сообществе.

```
Switch# show snmp community

Codes: ro - read only, rw - Read Write

Community      access view
-----
-
System         rw  sales-divison checked with IP access control list:
SalesDvision
public         ro  RD-division checked with IP access control list: HB5
Develop        ro  RD2
private        rw  Line2 checked with IP access control list: HQ

Total Entries: 4

Switch#
```

В данном примере показано, как отобразить настройки SNMP-сервера.

```

Switch# show snmp host

Host IP Address   : 10.20.30.40
SNMP Version     : V1
Community Name   : public
UDP Port         : 50001

Host IP Address   : 10.10.10.1
SNMP Version     : V3 noauthnopriv
SNMPv3 User Name : user1
UDP Port         : 50001

Host IPv6 Address: 1:12:123::100
SNMP Version     : V3 noauthnopriv
SNMPv3 User Name : user2
UDP Port         : 162

Total Entries: 3

Switch#

```

В данном примере показано, как отобразить настройки MIB View.

```

Switch# show snmp view

View Name          Subtree                View Type
-----
restricted         1.3.6.1.2.1.1          Included
restricted         1.3.6.1.2.1.11         Included
restricted         1.3.6.1.6.3.10.2.1     Included
restricted         1.3.6.1.6.3.11.2.1     Included
restricted         1.3.6.1.6.3.15.1.1     Included
CommunityView     1                      Included
CommunityView     1.3.6.1.6.3            Excluded
CommunityView     1.3.6.1.6.3.1         Included

Total Entries: 8

Switch#

```

В данном примере показано, как отобразить настройки SNMP-группы.

```

Switch# show snmp group

GroupName: public                               SecurityModel: v1
  ReadView    : CommunityView                   WriteView    :
  NotifyView  : CommunityView
IP access control list:

GroupName: public                               SecurityModel: v2c
  ReadView    : CommunityView                   WriteView    :
  NotifyView  : CommunityView
IP access control list:

GroupName: initial                             SecurityModel: v3/noauth
  ReadView    : restricted                       WriteView    :
  NotifyView  : restricted
IP access control list:

GroupName: private                             SecurityModel: v1
  ReadView    : CommunityView                   WriteView    : CommunityView
  NotifyView  : CommunityView
IP access control list:

GroupName: private                             SecurityModel: v2c
  ReadView    : CommunityView                   WriteView    : CommunityView
  NotifyView  : CommunityView
IP access control list:

Total Entries: 5

Switch#

```

В данном примере показано, как отобразить SNMP engine ID.

```

Switch# show snmp engineID

Local SNMP engineID: 800000ab033c1e04a1b9e000

Switch#

```

## 57-15 show snmp user

Данная команда используется для отображения информации о настроенном SNMP-пользователе.

**show snmp user** [USER-NAME]

**Параметры**

<i>USER-NAME</i>	(Опционально) Укажите имя SNMP-пользователя, о котором необходимо отобразить информацию.
------------------	--

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Если имя пользователя не указано, будут отображены все настроенные пользователи. С помощью данной команды нельзя отобразить созданную строку Community String.

**Пример**

В данном примере показано, как отобразить SNMP-пользователей.

```
Switch# show snmp user authuser

User name: authuser
  Security Model: v2c
  Group Name: VacmGroupName
IP access control list: HB5

User name: authuser
  Security Model: v3 priv
  Group Name: VacmGroupName
  Authentication Protocol: MD5
  Privacy Protocol: DES
  Engine ID: 0000000902000000C025808
IP access control list:

Total Entries: 2

Switch#
```

**57-16 snmp-server community**

Данная команда используется для настройки строки идентификатора сообщества (Community String) для доступа к SNMP. Используйте форму **no**, чтобы удалить строку Community String.

```
snmp-server community COMMUNITY-STRING [view VIEW-NAME] [ro | rw] [access IP-ACL-NAME]
no snmp-server community COMMUNITY-STRING
```



**Параметры**

<i>COMMUNITY-STRING</i>	Указывает сообщество, содержащее максимум 32 буквенно-цифровых символа.
<b>view</b> <i>VIEW-NAME</i>	(Опционально) Укажите имя ранее настроенного View, которое доступно указанному SNMP-сообществу.
<b>ro</b>	(Опционально) Укажите право «только чтение».
<b>rw</b>	(Опционально) Укажите право «чтение/запись».
<b>access</b> <i>IP-ACL-NAME</i>	(Опционально) Укажите имя стандартного списка доступа, дающего возможность пользователю использовать указанную строку Community String при доступе к агенту SNMP. Укажите доступного пользователя в поле адреса источника записи списка доступа.

**По умолчанию**

<b>Community</b>	<b>View Name</b>	<b>Access right</b>
private	CommunityView	Read/Write (чтение/запись)
public	CommunityView	Read Only (только чтение)

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Данная команда предоставляет простой способ для создания строки Community String для управления SNMPv1 и SNMPv2c. При создании сообщества с помощью команды **snmp-server community** будут созданы две записи SNMP-группы: одна для SNMPv1 и другая для SNMPv2c, у которых имя сообщества совпадают с именами групп. Если View не указан, разрешен доступ ко всем объектам.

**Пример**

В данном примере показано, как создать MIB View «interfacesMibView» и строку Community String «comaccess», с помощью которой можно получить право «чтение/запись» к созданному View «interfacesMibView».

```
Switch# configure terminal
Switch(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)# snmp-server community comaccess view interfacesMibView rw
Switch(config)#
```

**57-17 snmp-server engineID local**

Данная команда используется для указания SNMP engine ID на локальном устройстве. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
snmp-server engineID local ENGINEID-STRING
no snmp-server engineID local
```

**Параметры**

<i>ENGINEID-STRING</i>	Укажите строку engine ID. Максимально допустимое количество символов в строке – 24.
------------------------	---

### По умолчанию

По умолчанию SNMP engine ID генерируется автоматически.

### Режим ввода команды

Global Configuration Mode

### Использование команды

SNMP engine ID, уникальная строка для идентификации устройства, не отображается и не хранится в текущей конфигурации. По умолчанию строка генерируется автоматически. Строка, количество символов в которой менее 24, будет дополнена нулями, так чтобы общее количество символов составило 24.

### Пример

В данном примере показано, как настроить SNMP engine ID со значением 332200000000000000000000.

```
Switch# configure terminal
Switch(config)# snmp-server engineID local 332200000000000000000000
Switch(config)#
```

## 57-18 snmp-server group

Данная команда используется для настройки SNMP-группы. Используйте форму **no**, чтобы удалить SNMP-группу или удалить группу из используемой указанной модели безопасности.

```
snmp-server group GROUP-NAME {v1 | v2c | v3 {auth | noauth | priv}} [read READ-VIEW] [write WRITE-VIEW] [notify NOTIFY-VIEW] [access IP-ACL-NAME]
no snmp-server group GROUP-NAME {v1 | v2c | v3 {auth | noauth | priv}}
```

### Параметры

<i>GROUP-NAME</i>	Укажите имя группы. Максимально допустимое количество символов в строке – 32. Пробелы в строке недопустимы.
<b>v1</b>	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv1.
<b>v2c</b>	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv2c.
<b>v3</b>	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv3.
<b>auth</b>	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv3.
<b>noauth</b>	Укажите для отмены аутентификации и шифрования пакетов.
<b>priv</b>	Укажите для аутентификации и шифрования пакетов.
<b>read</b> <i>READ-VIEW</i>	(Опционально) Укажите, чтобы обеспечить доступ на чтение пользователю данной группы.

<b>write</b> <i>WRITE-VIEW</i>	(Опционально) Укажите, чтобы обеспечить доступ на запись пользователю данной группы.
<b>notify</b> <i>NOTIFY-VIEW</i>	(Опционально) Укажите, чтобы обеспечить доступ для уведомлений пользователю данной группы. В данном уведомлении описывается объект, о состоянии которого пользователь данной группы узнает с помощью SNMP trap.
<b>access</b> <i>IP-ACL-NAME</i>	(Опционально) Укажите стандартный IP-адрес списка управления доступом (ACL) для ассоциирования с группой.

#### По умолчанию

Group Name	Version	Security Level	Read View Name	Write View Name	Notify View
Initial	SNMPv3	noauth	Restricted	None	Restricted
ReadGroup	SNMPv1	None	CommunityView	None	CommunityView
ReadGroup	SNMPv2c	None	CommunityView	None	CommunityView
WriteGroup	SNMPv1	None	CommunityView	CommunityView	CommunityView
WriteGroup	SNMPv2c	None	CommunityView	CommunityView	CommunityView

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Для определения пользователя SNMP-группы необходимо указать разрешенную модель безопасности и право с помощью параметров *READ-VIEW*, *WRITE-VIEW* и *NOTIFY-VIEW*. Модель безопасности позволяет пользователю использовать указанную версию SNMP при доступе к агенту SNMP.

Возможно создание групп с одинаковыми именами при указании разных моделей безопасности SNMPv1, SNMPv2c и SNMPv3 одновременно. При указании SNMPv3 доступно использование двух параметров **auth** и **priv** одновременно.

Чтобы загрузить новый профиль View для группы для определенной модели безопасности, удалите ранее созданную группу и создайте новую группу с новым профилем View.

Параметр *READ-VIEW* определяет MIB-объекты, которые доступны для чтения пользователю группы. Если *READ-VIEW* не указан, может быть прочитано Internet OID-пространство 1.3.6.1.

Параметр *WRITE-VIEW* определяет MIB-объекты, которые доступны для записи пользователю группы. Если *WRITE-VIEW* не указан, никакой из MIB-объектов не может быть записан.

Параметр *NOTIFY-VIEW* определяет MIB-объекты, с помощью которых система может сообщать о своем статусе в notify-пакетах уведомлений trap-менеджерам, которые идентифицированы указанным пользователем группы, выступающим в качестве строки Community String. Если *NOTIFY-VIEW* не указан, информация о MIB-объектах не будет получена.

#### Пример

В данном примере показано, как создать группу SNMP-сервера для доступа по SNMPv3 и SNMPv2c. Настроенная группа – guestgroup.

```
Switch# configure terminal
Switch(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)# snmp-server group guestgroup v3 auth read interfacesMibView
Switch(config)# snmp-server group guestgroup v2c read CommunityView write CommunityView
Switch(config)#
```

## 57-19 snmp-server host

Данная команда используется для указания получателя SNMP-уведомлений. Используйте форму **no**, чтобы удалить получателя.

```
snmp-server host {IP-ADDRESS | IPV6-ADDRESS} [version {1 | 2c | 3 {auth | noauth | priv}}]
COMMUNITY-STRING [port PORT-NUMBER]
no snmp-server host {IP-ADDRESS | IPV6-ADDRESS}
```

### Параметры

<i>IP-ADDRESS</i>	Укажите IPv4-адрес узла-получателя сервера для SNMP - уведомлений.
<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес узла-получателя сервера для SNMP-уведомлений.
<b>version</b>	(Опционально) Укажите версию SNMP, которую необходимо использовать для отправки SNMP trap. Если версия не указана, по умолчанию используется SNMPv1. <b>1</b> – SNMPv1. <b>2c</b> – SNMPv2c. <b>3</b> – SNMPv3.
<b>auth</b>	(Опционально) Укажите для аутентификации пакетов. Данный параметр не используется для шифрования пакетов.
<b>noauth</b>	Укажите для отмены аутентификации и шифрования пакетов.
<b>priv</b>	Укажите для аутентификации и шифрования пакетов.
<i>COMMUNITY-STRING</i>	Введите строку Community String, которую необходимо отправить с notify- пакетами уведомлений. При указании версии 3 строка Community String используется в качестве имени пользователя, как показано в примере команды <b>snmp-sever user</b> .
<b>port</b> <i>PORT-NUMBER</i>	(Опционально) Укажите номер UDP-порта. Номер UDP-порта trap по умолчанию – 162. Доступный диапазон номеров UDP-порта: от 1 до 65535. Некоторые номера портов могут конфликтовать с другими протоколами.

### По умолчанию

По умолчанию используется версия 1.

### Режим ввода команды

Global Configuration Mode

## Использование команды

SNMP-уведомления отправляются в виде SNMP trap. Для отправки SNMP-уведомлений необходимо создать по крайней мере одного получателя при помощи команды **snmp-server host**. Для созданного пользователя укажите версию SNMP trap-пакетов. При указании SNMPv1 и SNMPv2c уведомления SNMP trap будут отправлены в PDU (Trap Protocol Data Unit). При указании SNMPv3 уведомления SNMP trap будут отправлены в SNMPv2-TRAP-PDU с заголовком SNMPv3.

При указании SNMPv1 или SNMPv2c для отправки SNMP trap на определенный узел указанная строка Community String выступает в качестве строки SNMP trap.

При указании SNMPv3 для отправки SNMP trap на определенный узел укажите, необходима ли аутентификация и шифрование отправленных пакетов. Указанная строка Community String выступает в качестве имени пользователя в пакетах SNMPv3. При использовании команд **snmp-server user** или **snmp-server user v3** сначала необходимо создать пользователя.

При отправке SNMP trap система проверит уведомления View, ассоциированные с указанным пользователем или именем сообщества. Если переменные привязки (Binding Variables), которые должны быть отправлены с SNMP trap, отсутствуют в уведомлениях View, уведомления не будут отправлены на данный сервер.

## Пример

В данном примере показано, как настроить SNMP trap-получателя с указанием версии 1 и со строкой Community String «comaccess». SNMP trap-получатель – 163.10.50.126.

```
Switch# configure terminal
Switch(config)# snmp-server community comaccess rw
Switch(config)# snmp-server host 163.10.50.126 version 1 comaccess
Switch(config)#
```

В данном примере показано, как настроить SNMP trap-получателя с указанием типа уровня безопасности аутентификации версии 3 и имени пользователя «useraccess». SNMP trap-получатель – 163.10.50.126.

```
Switch# configure terminal
Switch(config)# snmp-server group groupaccess v3 auth read CommunityView write CommunityView
Switch(config)# snmp-server user useraccess groupaccess v3 auth md5 12345678
Switch(config)# snmp-server host 163.10.50.126 version 3 auth useraccess
Switch(config)#
```

В данном примере показано, как настроить SNMP trap-получателя с указанием версии 1 и со строкой Community String «comaccess». SNMP trap-получатель – 163.10.50.126. Номер UDP-порта – 50001.

```
Switch# configure terminal
Switch(config)# snmp-server community comaccess rw
Switch(config)# snmp-server host 163.10.50.126 version 1 comaccess port 50001
Switch(config)#
```

## 57-20 snmp-server user

Данная команда используется для создания SNMP-пользователя. Используйте форму **no**, чтобы удалить SNMP-пользователя.

**snmp-server user** USER-NAME GROUP-NAME {v1 | v2c | v3 [encrypted] [auth {md5 | sha} AUTH-PASSWORD [priv PRIV-PASSWORD ]]} [access IP-ACL-NAME]

**no snmp-server user** *USER-NAME GROUP-NAME {v1| v2c | v3}*

#### Параметры

<i>USER-NAME</i>	Укажите имя пользователя. Максимально допустимое количество символов в строке – 32. Пробелы в строке недопустимы.
<i>GROUP-NAME</i>	Укажите имя группы, к которой принадлежит данный пользователь. Пробелы в строке недопустимы.
<b>v1</b>	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv1.
<b>v2c</b>	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv2c.
<b>v3</b>	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv3.
<b>encrypted</b>	(Опционально) Укажите для шифрования пароля.
<b>auth</b>	(Опционально) Укажите тип аутентификации.
<b>md5</b>	(Опционально) Укажите использование аутентификации MAC-MD5-96.
<b>sha</b>	(Опционально) Укажите использование аутентификации HMAC-SHA-96.
<i>AUTH-PASSWORD</i>	(Опционально) Укажите пароль аутентификации в форме обычного текста. Для MD5 пароль может содержать от 8 до 16 символов, для SHA – от 8 до 20. При указании параметра <b>encrypted</b> длина пароля для MD5 составляет 32, для SHA – 40. В данном параметре используются шестнадцатеричные значения.
<b>priv</b>	(Опционально) Укажите тип шифрования.
<i>PRIV-PASSWORD</i>	Укажите пароль Private в форме обычного текста. Максимально допустимое количество символов – 64. При указании параметра <b>encrypted</b> фиксированная длина пароля – 16 символов.
<b>access</b> <i>IP-ACL-NAME</i>	(Опционально) Укажите стандартный IP-адрес ACL для ассоциирования с пользователем.

#### По умолчанию

По умолчанию настроен один пользователь.

**Имя пользователя** – initial.

**Имя группы** – initial.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Для создания SNMP-пользователя укажите модель безопасности, которая будет использована данным пользователем, и группу, для которой создан данный пользователь. Для создания SNMPv3-пользователя необходимо указать пароль для аутентификации и шифрования.

Невозможно удалить SNMP-пользователя, который был ассоциирован с SNMP-сервером.

### Пример

В данном примере показано, как настроить пароль в форме обычного текста для пользователя «user1» в группе «public» в версии SNMPv3.

```
Switch# configure terminal
Switch(config)# snmp-server user user1 public v3 auth md5 authpassword priv privpassword
Switch(config)#
```

В данном примере показано, как использовать строку MD5 digest вместо пароля в форме обычного текста.

```
Switch# configure terminal
Switch(config)# snmp-server user user1 public v3 encrypted auth md5
00112233445566778899AABBCCDDEEFF
Switch(config)#
```

## 57-21 snmp-server view

Данная команда используется для создания или изменения записи View. Используйте форму по, чтобы удалить указанную запись SNMP View.

**snmp-server view** VIEW-NAME OID-TREE {included | excluded}  
**no snmp-server view** VIEW-NAME

### Параметры

<b>VIEW-NAME</b>	Указывает имя записи представления. Допустимая длина - от 1 до 32 символов. Синтаксис - общая строка, не допускающая пробелов.
<b>OID-TREE</b>	Указывает идентификатор объекта sub-tree ASN.1, которое должно быть включено или исключено из представления. Для идентификации sub-tree укажите текстовую строку, состоящую из чисел, например 1.3.6.2.4, или слово, например system. Используйте подстановочный знак звездочки (*) в одном sub-identifier, чтобы указать семейство sub-tree.
<b>included</b>	Указывает sub-tree, которое должно быть включено в представление SNMP.
<b>excluded</b>	Указывает sub-tree, которое должно быть исключено из представления SNMP.

### По умолчанию

VIEW-NAME	OID-TREE	View Type
Restricted	1.3.6.1.2.1.1	Included
Restricted	1.3.6.1.2.1.11	Included
Restricted	1.3.6.1.6.3.10.2.1	Included
Restricted	1.3.6.1.6.3.11.2.1	Included
Restricted	1.3.6.1.6.3.15.1.1	Included
CommunityView	1	Included

CommunityView	1.3.6.1.6.3	Excluded
CommunityView	1.3.6.1.6.3.1	Included

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду, чтобы создать View MIB-объектов.

### Пример

В данном примере показано, как создать MIB View и предоставить доступ для чтения SNMP-группе, ассоциированной с данным MIB View. Настроенный MIB View – interfacesMibView. SNMP-группа – guestgroup.

```
Switch# configure terminal
Switch(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)# snmp-server group guestgroup v3 auth read interfacesMibView
Switch(config)#
```



## 58. Команды Spanning Tree Protocol (STP)

### 58-1 clear spanning-tree detected-protocols

Данная команда используется для перезапуска процесса миграции протокола.

```
clear spanning-tree detected-protocols {all | interface INTERFACE-ID}
```

#### Параметры

<b>all</b>	Укажите, чтобы запустить действие обнаружения для всех портов.
<i>INTERFACE-ID</i>	Укажите интерфейс порта, на котором необходимо запустить действие обнаружения.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

С помощью данной команды во время миграции протокола порт будет переведен в состояние *SEND\_RSTP*. Данное действие можно использовать, чтобы проверить, все ли устаревшие мосты на LAN были удалены. При отсутствии моста STP на данной LAN порт будет работать в выбранном режиме RSTP или MSTP. В противном случае порт будет работать в режиме STP.

#### Пример

В данном примере показано, как запустить процесс миграции протокола для всех портов.

```
Switch# clear spanning-tree detected-protocols all
Clear spanning-tree detected-protocols? (y/n) [n] y
Switch#
```

### 58-2 show spanning-tree

Данная команда используется для отображения информации о работе протокола Spanning Tree и применяется только для STP и RSTP.

```
show spanning-tree [interface [INTERFACE-ID [, | -]]]
```

#### Параметры

<b>interface</b> <i>INTERFACE-ID</i>	(Опционально) Укажите ID интерфейса, который необходимо отобразить.
--------------------------------------	---

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

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте данную команду для отображения настроек Spanning Tree одного связующего дерева в режиме, совместимом с RSTP или STP.

**Пример**

В данном примере показано, как отобразить информацию о Spanning Tree при включенном STP.

```
Switch# show spanning-tree

Spanning Tree: Enabled
Protocol Mode: RSTP
Tx-hold-count: 6
Root ID Priority: 32768
    Address: 3C-1E-04-A1-B9-E0
    Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
Bridge ID Priority: 32768 (priority 32768 sys-id-ext 0)
    Address: 3C-1E-04-A1-B9-E0
    Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec,
Topology Changes Count: 0

Interface      Role      State      Cost      Priority Link
-----      ----      -
eth1/0/3      designated forwarding 20000      128.3      p2p      non-edge
eth1/0/5      backup    blocking   200000     128.5      p2p      non-edge
eth1/0/6      backup    blocking   200000     128.6      shared  non-edge
eth1/0/7      root      forwarding 2000       128.7      P2p      non-edge

Switch#
```

**58-3 show spanning-tree configuration interface**

Данная команда используется для отображения информации о настройках интерфейса STP.

**show spanning-tree configuration interface [INTERFACE-ID [, | -]]**

#### Параметры

<i>INTERFACE-ID</i>	(Опционально) Укажите ID интерфейса, который необходимо отобразить.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте данную команду для отображения настроек интерфейса Spanning Tree. Команда может быть использована для всех версий STP.

#### Пример

В данном примере показано, как отобразить информацию о настройках Spanning Tree для интерфейса Ethernet 1/0/1.

```
Switch#show spanning-tree configuration interface ethernet 1/0/1

eth1/0/1
Spanning tree state : Enabled
Port path cost: 0
Port priority: 128
Port Identifier: 128.1
Link type: auto
Port fast: edge
Guard root: Disabled
TCN filter : Disabled
Bpdu forward: Disabled

Switch#
```

## 58-4 snmp-server enable traps stp

Данная команда используется для включения отправки SNMP-уведомлений для STP. Используйте форму **no**, чтобы отключить отправку уведомлений для STP.

**snmp-server enable traps stp [new-root] [topology-chg]**

**no snmp-server enable traps stp [new-root] [topology-chg]****Параметры**

<b>new-root</b>	(Опционально) Укажите для отправки уведомлений о новом корне STP.
<b>topology-chg</b>	(Опционально) Укажите для отправки уведомлений об изменении STP- топологии.

**По умолчанию**

По умолчанию данная функция отключена.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Используйте данную команду, чтобы включить/отключить отправку trap-уведомлений. Если ни один из опциональных параметров не указан в форме **no** данной команды, будут отключены оба типа уведомлений STP.

**Пример**

В данном примере показано, как включить отправку всех STP trap на узел 10.9.18.100, используя строку сообщества «public».

```
Switch# configure terminal
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server enable traps stp
Switch(config)# snmp-server host 10.9.18.100 version 2c public
Switch(config)#
```

**58-5 spanning-tree global state**

Данная команда используется для включения/отключения глобального состояния STP. Используйте форму **no**, чтобы отключить глобальное состояние STP.

**spanning-tree global state {enable | disable}**  
**no spanning-tree global state**

**Параметры**

<b>enable</b>	Укажите, чтобы включить глобальное состояние STP.
<b>disable</b>	Укажите, чтобы отключить глобальное состояние STP.

**По умолчанию**

По умолчанию данная функция отключена.

**Режим ввода команды**

Global Configuration Mode

### Использование команды

Используйте данную команду в режиме Global Configuration Mode, чтобы включить функцию Spanning Tree глобально.

### Пример

В данном примере показано, как включить функцию Spanning Tree.

```
Switch# configure terminal
Switch(config)# spanning-tree global state enable
Switch(config)#
```

## 58-6 spanning-tree (timers)

Данная команда используется для настройки значений таймеров Spanning Tree. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
spanning-tree {hello-time SECONDS | forward-time SECONDS | max-age SECONDS}
no spanning-tree {hello-time | forward-time | max-age}
```

### Параметры

<b>hello-time SECONDS</b>	Укажите интервал между циклической передачей конфигурационных сообщений. Доступный диапазон значений: от 1 до 2 секунд.
<b>forward-time SECONDS</b>	Укажите время задержки продвижения (Forward Delay), используемое STP для перехода из состояния Listening и Learning в состояние Forwarding. Доступный диапазон значений: от 4 до 30 секунд.
<b>max-age SECONDS</b>	Укажите максимальное время жизни сообщения BPDU. Доступный диапазон значений: от 6 до 40 секунд.

### По умолчанию

Значение параметра **hello-time** по умолчанию – 2 секунды.

Значение параметра **forward-time** по умолчанию – 15 секунд.

Значение параметра **max-age no** по умолчанию – 20 секунд.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду, чтобы настроить значения таймеров Spanning Tree.

### Пример

В данном примере показано, как настроить значения таймеров Spanning Tree.

```
Switch# configure terminal
Switch(config)# spanning-tree hello-time 1
Switch(config)# spanning-tree forward-time 16
Switch(config)# spanning-tree max-age 21
Switch(config)#
```

## 58-7 spanning-tree state

Данная команда используется для включения /отключения STP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**spanning-tree state {enable | disable}**  
**no spanning-tree state**

### Параметры

<b>enable</b>	Укажите, чтобы включить STP для настраиваемого интерфейса.
<b>disable</b>	Укажите, чтобы отключить STP для настраиваемого интерфейса.

### По умолчанию

По умолчанию эта функция включена.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Если Spanning Tree включено, BPDU, полученный портом, будет либо отправлен, либо обработан. Используя данную команду, не допускайте появления петель. Данная команда не будет применена, если функция L2PT включена для STP.

### Пример

В данном примере показано, как включить Spanning Tree на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# spanning-tree state enable
Switch(config-if)#
```

## 58-8 spanning-tree cost

Данная команда используется для настройки значения стоимости пути на указанном порту. Используйте форму **no**, чтобы определить стоимость пути автоматически.

**spanning-tree cost COST**  
**no spanning-tree cost**

### Параметры

---

**COST**Укажите стоимость пути для порта. Доступный диапазон значений: от 1 до 200000000.

---

**По умолчанию**

По умолчанию стоимость пути определяется на основе настроек полосы пропускания интерфейса.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

В режимах, совместимых с STP и RSTP, для одного связующего дерева стоимость пути, заданная администратором, используется для достижения корня (Root). В режиме MSTP региональным корнем CIST (CIST Regional Root) используется стоимость пути, заданная администратором, для достижения корня CIST (CIST Root).

**Пример**

В данном примере показано, как настроить значение стоимости пути на интерфейсе Ethernet 1/0/7. Настроенное значение: 20000.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/7
Switch(config-if)# spanning-tree cost 20000
Switch(config-if)#
```

**58-9 spanning-tree guard root**

Данная команда используется для включения функции STP Root Guard. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**spanning-tree guard root**  
**no spanning-tree guard root**

**Параметры**

Нет

**По умолчанию**

По умолчанию данная функция отключена.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

BPDU Guard предотвращает превращение порта в корневой порт и ограничивает доступ внешним мостам, находящимся не под полным контролем администратора, к основному региону сети активной топологии связующего дерева.

Порт, которому было отказано в присвоении роли корневого порта (Root Port), сможет работать только в качестве назначенного порта (Designated Port). При получении конфигурационного BPDU с более высоким приоритетом порт начнет работать в качестве альтернативного порта (Alternate Port) в состоянии «Blocking». Получение BPDU с более высоким приоритетом не повлияет на построение STP. Порт будет прослушивать сообщения BPDU. Если время ожидания получения BPDU с наибольшим приоритетом истечет, порт начнет работать в качестве назначенного порта.

Когда функция Guard Root сработает и порт начнет работать в качестве альтернативного порта, будет сгенерировано системное сообщение. Данные настройки действительны для всех версий Spanning Tree.

### Пример

В данном примере показано, как предотвратить смену роли порта на роль корневого порта (Root port) для интерфейса Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# spanning-tree guard root
Switch(config-if)#
```

## 58-10 spanning-tree link-type

Данная команда используется для настройки типа соединения (Link-type) для порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**spanning-tree link-type {point-to-point | shared}**  
**no spanning-tree link-type**

### Параметры

<b>point-to-point</b>	Укажите тип соединения «точка-точка» (Point To Point, P2P).
<b>shared</b>	Укажите тип соединения для подключения к сети общего пользования (Shared Media).

### По умолчанию

Если ни один из параметров не указан, тип соединения по умолчанию назначается на основе настроек дуплекса.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

На портах, функционирующих в режиме полного дуплекса, устанавливается соединение Point To Point; порты, работающие в режиме полудуплекса, считаются портами общего пользования (Shared Port). Так как быстрый переход в состояние Forwarding при использовании типа соединения Shared Media невозможен, рекомендуется использовать автоматическое определение Link-type модулем STP.

Данные настройки действительны для всех режимов Spanning Tree.



## Пример

В данном примере показано, как настроить тип соединения Point To Point для Ethernet-порта 1/0/7.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/7
Switch(config-if)# spanning-tree link-type point-to-point
Switch(config-if)#
```

## 58-11 spanning-tree mode

Данная команда используется для настройки режима STP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
spanning-tree mode {mstp | rstp | stp}
no spanning-tree mode
```

### Параметры

<b>mstp</b>	Укажите Multiple Spanning Tree Protocol (MSTP).
<b>rstp</b>	Укажите Rapid Spanning Tree Protocol (RSTP).
<b>stp</b>	Укажите Spanning Tree Protocol (совместимый с IEEE 802.1D).

### По умолчанию

Режим по умолчанию – RSTP.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Если настраивается режим STP или RSTP, все текущие MSTP-экземпляры будут отменены автоматически. При изменении режима Spanning Tree все порты перейдут в состояние Discarding (отбрасывание).

## Пример

В данном примере показано, как настроить текущую версию протокола STP на RSTP.

```
Switch# configure terminal
Switch(config)# spanning-tree mode rstp
Switch(config)#
```

## 58-12 spanning-tree portfast

Данная команда используется для настройки режима Port Fast на порту. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
spanning-tree portfast {disable | edge| network}
no spanning-tree portfast
```

**Параметры**

<b>disable</b>	Укажите для включения режима Fast Disable на порту.
<b>edge</b>	Укажите для включения режима Fast Edge на порту.
<b>network</b>	Укажите для включения режима Fast Network на порту.

**По умолчанию**

Режим по умолчанию – **Edge Mode**.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

На порту может быть установлен один из трех режимов Port Fast:

- **Edge Mode:** при установлении соединения порт сразу же переходит в состояние Forwarding, не дожидаясь задержки продвижения (Forward Delay). Рабочее состояние интерфейса, на котором BPDU было получено позже, будет изменено на состояние Non-Port-Fast.
- **Disable Mode:** порт всегда находится в состоянии Non-Port-Fast и будет ждать, пока Forward Delay не перейдет в состояние Forwarding.
- **Network Mode:** порт находится в состоянии Non-Port-Fast в течение трех секунд. Не получив BPDU, порт переходит в состояние Port-Fast, за которым следует состояние Forwarding. Состояние порта, на котором BPDU было получено позже, будет изменено на состояние Non-Port-Fast.

Применяя данную команду, не допускайте появления петель в топологии и петель во время передачи пакетов данных, которые нарушают работу сети.

**Пример**

В данном примере показано, как настроить режим Port-Fast Edge для Ethernet-порта 1/0/7.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/7
Switch(config-if)# spanning-tree portfast edge
Switch(config-if)#
```

**58-13 spanning-tree port-priority**

Данная команда используется для настройки значения приоритета STP на указанном порту. Команда применима только для версий RSTP и STP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
spanning-tree port-priority PRIORITY
no spanning-tree port-priority
```

**Параметры**

<b>PRIORITY</b>	Укажите приоритет порта в диапазоне от 0 до 240.
-----------------	--

**По умолчанию**

Значение по умолчанию – 128.

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

При присвоении роли порту используется его идентификатор, который состоит из приоритета и номера порта. Чем ниже число, тем выше приоритет. Данный параметр применим только в режимах RSTP или STP.

#### Пример

В данном примере показано, как настроить приоритет для Ethernet-порта 1/0/7 со значением 0.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/7
Switch(config-if)# spanning-tree port-priority 0
Switch(config-if)#
```

## 58-14 spanning-tree priority

Данная команда используется для настройки приоритета моста. Команда применима только для версий RSTP и STP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**spanning-tree priority** *PRIORITY*  
**no spanning-tree priority**

#### Параметры

<i>PRIORITY</i>	Укажите Bridge-ID Spanning Tree, который состоит из приоритета и MAC-адреса моста. Bridge-ID является важным фактором в топологии Spanning Tree. Доступный диапазон значений: от 0 до 61440.
-----------------	--

#### По умолчанию

Значение по умолчанию – 32768.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Выбор корневого моста зависит от значения приоритета моста и системного MAC-адреса. Значение приоритета моста должно делиться на 4096. Чем меньше число, тем выше приоритет.

Данные настройки применимы для версий STP и RSTP протокола Spanning Tree. В режиме MSTP используйте команду **spanning-tree mst priority**, чтобы настроить приоритет для MSTP-экземпляра.

#### Пример

В данном примере показано, как настроить приоритет моста STP со значением 4096.

```
Switch# configure terminal
Switch(config)# spanning-tree priority 4096
Switch(config)#
```

## 58-15 spanning-tree tcnfilter

Данная команда используется для включения фильтрации уведомлений об изменении топологии сети TCN (Topology Change Notification) на указанном интерфейсе. Используйте форму **no**, чтобы отключить фильтрацию TCN.

```
spanning-tree tcnfilter
no spanning-tree tcnfilter
```

### Параметры

Нет

### По умолчанию

По умолчанию данная функция отключена.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Фильтрация TCN используется для защиты ISP от подключения внешних мостов, находящихся не под полным контролем администратора, к основному региону сети, в котором в данной ситуации произойдет очистка (Flush) адресов.

В режиме фильтрации уведомление TCN об изменении топологии, полученное на порту, игнорируется. Данные настройки действительны для всех режимов Spanning Tree.

### Пример

В данном примере показано, как включить фильтрацию TCN на Ethernet-порту 1/0/7.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/7
Switch(config-if)# spanning-tree tcnfilter
Switch(config-if)#
```

## 58-16 spanning-tree tx-hold-count

Данная команда используется для ограничения максимального количества BPDU, которые могут быть отправлены перед паузой в одну секунду. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
spanning-tree tx-hold-count VALUE
no spanning-tree tx- hold-count
```

**Параметры**

<i>VALUE</i>	Укажите максимальное количество BPDU, которые могут быть отправлены перед паузой в одну секунду. Доступный диапазон значений: от 1 до 10.
--------------	---

**По умолчанию**

Значение по умолчанию – 6.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Используйте данную команду, чтобы указать максимальное количество отправляемых BPDU. Передача BPDU на порт контролируется счетчиком, значение которого увеличивается при каждой отправке BPDU и уменьшается раз в секунду. Передача BPDU приостанавливается на одну секунду, если счетчик достигает значения параметра Hold Count.

**Пример**

В данном примере показано, как настроить параметр Hold Count со значением 5.

```
Switch# configure terminal
Switch(config)# spanning-tree tx-hold-count 5
Switch(config)#
```

**58-17 spanning-tree forward-bpdu**

Данная команда используется для включения BPDU Forwarding в Spanning Tree. Используйте форму **no**, чтобы отключить BPDU Forwarding в Spanning Tree.

```
spanning-tree forward-bpdu
no spanning-tree forward-bpdu
```

**Параметры**

Нет

**По умолчанию**

По умолчанию данная функция отключена.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

При использовании данной команды полученные STP BPDU будут перенаправлены на все Member-порты VLAN без тега. Данная команда не будет применена, если функция L2PT включена для STP.

## Пример

В данном примере показано, как включить BPDU Forwarding в Spanning Tree.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# spanning-tree forward-bpdu
Switch(config-if)#
```

## 59. Команды Storm Control

### 59-1 snmp-server enable traps storm-control

Данная команда используется для включения и настройки отправки SNMP-уведомлений для Storm Control. Используйте форму **no**, чтобы отключить отставку SNMP-уведомлений.

```
snmp-server enable traps storm-control [storm-occur] [storm-clear]
no snmp-server enable traps storm-control [storm-occur] [storm-clear]
```

#### Параметры

<b>storm-occur</b>	(Опционально) Укажите для отправки уведомлений при возникновении шторма.
<b>storm-clear</b>	(Опционально) Укажите для отправки уведомлений при предотвращении шторма.

#### По умолчанию

По умолчанию данная функция отключена.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте эту команду, чтобы включить или отключить отставку уведомлений для управления storm. Если параметр не указан, включаются или отключаются оба параметра **storm-occur** и **storm-clear**.

#### Пример

В данном примере показано, как включить отставку trap-сообщений при возникновении и предотвращении шторма.

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

### 59-2 storm-control

Данная команда используется для защиты устройства от штормовых атак широковещательных и многоадресных пакетов или пакетов с неизвестным адресом назначения. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
storm-control {{broadcast | multicast | unicast} level {pps PPS-RISE [PPS-LOW] | kbps KBPS-RISE
[KBPS-LOW] | LEVEL-RISE [LEVEL-LOW]} | action {shutdown | drop | none}}
no storm-control {broadcast | multicast | unicast | action}
```

#### Параметры

<b>broadcast</b>	Укажите для ограничения скорости широковещательной рассылки.
<b>multicast</b>	Укажите для ограничения скорости многоадресной рассылки.
<b>unicast</b>	Укажите, чтобы в режиме <b>shutdown</b> применять команду как к известным, так и к неизвестным одноадресным пакетам. При достижении на порту установленного лимита пакетов порт будет отключен. Если указан другой режим, команда будет применена только к неизвестным одноадресным пакетам.
<b>level pps</b> <i>PPS-RISE</i> [ <i>PPS-LOW</i> ]	Укажите пороговое значение пакетов в секунду. Доступный диапазон значений: от 1 до 2147483647. Если минимальный уровень (Low Level) PPS не указан, значение по умолчанию составляет 80% от указанного максимального (Rise) PPS.
<b>level kbps</b> <i>KBPS-RISE</i> [ <i>KBPS-LOW</i> ]	Укажите пороговое значение скорости передачи трафика, полученного на порту, в битах в секунду. Доступный диапазон значений: от 1 до 2147483647. Если минимальный уровень (Low Level) KBPS не указан, значение по умолчанию составляет 80% от указанного максимального (Rise) KBPS.
<b>level</b> <i>LEVEL-RISE</i> [ <i>LEVEL-LOW</i> ]	Укажите пороговое значение трафика, полученного на порту, в процентах от общей пропускной способности. Доступный диапазон значений: от 1 до 100. Если минимальный уровень (Low Level) не указан, значение по умолчанию составляет 80% от указанного максимального уровня (Rise Level).
<b>action shutdown</b>	Укажите, чтобы отключить порт при достижении указанного максимального порогового значения.
<b>action drop</b>	Укажите, чтобы отбросить пакеты, которые превышают максимальный порог.
<b>action none</b>	Укажите, чтобы не фильтровать Storm пакеты.

### По умолчанию

Storm Control широковещательной, многоадресной и одноадресной (DLF) рассылки по умолчанию отключен. При возникновении шторма по умолчанию Storm пакеты будут отброшены.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Используйте функцию управления штормом для защиты сети от шторма широковещательных пакетов, пакетов многоадресной рассылки или неизвестных пакетов DA flooding. Введите команду storm-control, чтобы включить управление штормом для определенного типа трафика на интерфейсе.

Существует два способа восстановления отключенного в результате ошибки порта.

- Пользователь может использовать команду **errdisable recovery cause**, чтобы включить автоматическое восстановление портов, которые были отключены в результате штормового контроля.



- Пользователь может вручную восстановить порт, введя команду **shutdown**, а затем команду **no shutdown** для порта.

На интерфейсе может действовать только один режим счетчика (процент, kbps или pps). На интерфейсе, если последующий указанный параметр режима счетчика отличается от предыдущего режима, предыдущие настроенные штормы сбрасываются в состояние по умолчанию (отключено в данной спецификации).

Из-за аппаратных ограничений, когда режим счетчика - процент или кбит/с:

- Действие не может быть указано для режима отключения.
- Нет трапов и журналов для режимов drop и none.

Эта функция не может дать точный уровень подавления общей пропускной способности в процентах (от 0 до 100) для конкретного интерфейса порта. Текущая формула расчета предполагает, что размер пакета составляет 64 байта.

### Пример

В этом примере показано, как включить управление ширококестельным штормом на портах 1 и 2. Он устанавливает порог для порта 1 на 500 пакетов в секунду с помощью действия shutdown и устанавливает порог для порта 2 между 60% и 70% с помощью действия drop.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# storm-control broadcast level pps 500
Switch(config-if)# storm-control action shutdown
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# storm-control broadcast level 70 60
Switch(config-if)# storm-control action drop
Switch(config-if)#
```

## 59-3 storm-control polling

Данная команда используется для настройки интервала опроса (Polling Interval) для подсчета количества полученных пакетов. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**storm-control polling {interval SECONDS | retries {NUMBER | infinite}}**  
**no storm-control polling {interval | retries}**

### Параметры

<b>interval SECONDS</b>	Укажите интервал опроса для подсчета количества полученных пакетов. Доступный диапазон значений: от 1 до 300 секунд.
<b>retries NUMBER</b>	Укажите количество попыток интервалов между запросами. Если в режиме <b>shutdown</b> шторм продолжается во время установленных значений попыток, порт перейдет в состояние Error-Disabled. Доступный диапазон значений: от 0 до 360. 0 означает, что при обнаружении шторма порт в режиме <b>shutdown</b> сразу же будет отключен из-за ошибки. <b>Infinite</b> означает, что порт в режиме <b>shutdown</b> не будет отключен из-за ошибки даже при обнаружении шторма.

**По умолчанию**

Интервал опроса по умолчанию – 5 секунд.

Количество попыток по умолчанию – 3.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Используйте данную команду, чтобы указать интервал выборки для подсчета количества полученных пакетов.

**Пример**

В данном примере показано, как указать интервал опроса на 15 секунд.

```
Switch# configure terminal
Switch(config)# storm-control polling interval 15
Switch(config)#
```

**59-4 show storm-control**

Данная команда используется для отображения текущих настроек функции Storm Control.

**show storm-control interface *INTERFACE-ID* [, | -] [broadcast | multicast | unicast]**

**Параметры**

<b>interface</b> <i>INTERFACE-ID</i>	Укажите интервал опроса для подсчета количества полученных пакетов. Доступный диапазон значений: от 1 до 300 секунд.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
<b>broadcast</b>	(Опционально) Укажите, чтобы отобразить текущие настройки шторма широковещательных пакетов (Broadcast Storm).
<b>multicast</b>	(Опционально) Укажите, чтобы отобразить текущие настройки шторма многоадресных пакетов (Multicast Storm).
<b>unicast</b>	(Опционально) Укажите, чтобы отобразить текущие настройки шторма одноадресных пакетов (DLF).

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Если ID интерфейса не указан, будут отображены настройки всех интерфейсов. Если тип пакета не указан, будут отображены настройки всех типов Storm Control.

**Пример**

В данном примере показано, как отобразить текущие настройки Storm Control для широковещательных пакетов.

```
Switch# show storm-control interface ethernet 1/0/1-1/0/6 broadcast
```

Interface	Action	Threshold	Current	State
eth1/0/1	Drop	500/300 pps	200 pps	Forwarding
eth1/0/2	Drop	80/64 %	20 %	Forwarding
eth1/0/3	Drop	80/64 %	70 %	Dropped
eth1/0/4	Shutdown	50/50 %	20 %	Forwarding
eth1/0/5	None	50000/50000 kbps	2000 kbps	Forwarding
eth1/0/6	None	-	-	Inactive

```
Total Entries: 6
Switch#
```

В этом примере показано, как отобразить все типы настроек управления штормом на портах 1 - 2.

```
Switch# show storm-control interface eth1/0/1-2
```

```

Polling Interval      : 15 sec           Shutdown Retries     : Infinite
Trap                  : Disabled

```

Interface	Storm	Action	Threshold	Current	State
eth1/0/1	Broadcast	Drop	80/64 %	50%	Forwarding
eth1/0/1	Multicast	Drop	80/64 %	50%	Forwarding
eth1/0/1	Unicast	Drop	80/64 %	50%	Forwarding
eth1/0/2	Broadcast	Shutdown	500/300 pps	-	Error Disabled
eth1/0/2	Multicast	Shutdown	500/300 pps	-	Error Disabled
eth1/0/2	Unicast	Shutdown	500/300 pps	-	Error Disabled

```
Total Entries: 6
Switch#
```

**Отображаемые параметры**

<b>Interface</b>	ID интерфейса.
<b>Action</b>	Настраиваемые действия. Возможны следующие действия: Drop (отбрасывание), Shutdown (отключение), None (без действия).

<b>Threshold</b>	Настраиваемое пороговое значение.
<b>Current</b>	Фактическая текущая скорость трафика, которая проходит через интерфейс, единицей которой могут быть проценты, кбит/с, PPS в зависимости от настроенного режима. Аппаратно скорость может быть подсчитана только в PPS, приблизительно равного значению в процентах и кбит/с.
<b>State</b>	Текущее состояние Storm Control на указанном интерфейсе для данного типа трафика. Возможны следующие состояния: <b>Forwarding:</b> шторма не обнаружено. <b>Dropped:</b> шторм обнаружен, и штормовой трафик, превышающий пороговое значение, отбрасывается. <b>Error Disabled:</b> порт отключен из-за шторма. <b>Link Down:</b> порт физически отключен. <b>Inactive:</b> Storm Control не включен для данного типа трафика.

## 60. Команды Surveillance VLAN

### 60-1 surveillance vlan

Данная команда используется для глобального включения функции Surveillance VLAN и ее настройки. Используйте форму **no**, чтобы отключить функцию Surveillance VLAN.

```
surveillance vlan VLAN-ID
no surveillance vlan
```

#### Параметры

<i>VLAN-ID</i>	Укажите VLAN ID Surveillance VLAN в диапазоне от 2 до 4094.
----------------	---

#### По умолчанию

По умолчанию данная функция отключена.

#### Режим ввода команды

Global Configuration Mode

#### Уровень команды по умолчанию

Уровень 12

#### Использование команды

Используйте эту команду, чтобы включить глобальную функцию VLAN наблюдения и указать VLAN наблюдения на коммутаторе. Коммутатор имеет только одну сеть Surveillance VLAN. Эта сеть наблюдения VLAN также поддерживает распознавание устройств наблюдения, таких как IP-камеры (IPC) и сетевые видеорегистраторы (NVR), с помощью протокола ONVIF.

Команда **surveillance vlan** в режиме глобальной конфигурации и команда **surveillance vlan enable** в режиме конфигурации интерфейса должны быть включены для порта, чтобы запустить функцию surveillance VLAN.

Когда для порта включена сеть наблюдения VLAN, порт автоматически будет изучен как нетегированный член сети наблюдения VLAN. Полученные нетегированные пакеты наблюдения будут пересылаться в сети наблюдения VLAN. Полученные пакеты определяются как пакеты наблюдения, если MAC-адреса источников пакетов соответствуют OUI-адресам, настроенным командой **surveillance vlan mac-address**.

Сеть автоматического наблюдения VLAN также может использоваться для передачи видеотрафика от IP-камеры и связанных с ней компонентов, таких как серверы управления видео (VMS), клиенты VMS и видеокодеры. Эти устройства могут быть распознаны по адресу OUI и протоколу ONVIF. Если IPC распознается протоколом ONVIF, коммутатор узнает IPC на порту путем snooping Hello/ProbeMatch пакетов и затем включает порт в сеть VLAN видеонаблюдения.

Коммутатор рассматривает хост как сетевой видеорегистратор, когда он подключается к IPC через HTTP, HTTPS или RTSP. Коммутатор распознает сетевой видеорегистратор на этом порту и перемещает его в сеть VLAN наблюдения до тех пор, пока не закончится срок действия сработавшего механизма старения или не будет удален кабель LAN.

Когда хост отправляет ARP-запрос на IPC, коммутатор по-прежнему рассматривает хост как сетевой видеорегистратор, но только временно перемещает его в виртуальную локальную сеть наблюдения. Хост будет автоматически перемещен из VLAN наблюдения примерно через 30 секунд, если он больше не распознается как NVR.



**Примечание:** Один и тот же ПК или ПК, подключенные к одному порту LAN на коммутаторе, не могут одновременно управлять коммутатором и подключенными к нему IP-камерами.

Если IPC распознан по OUI-адресу, коммутатор определит, является ли полученный пакет видеофайлом или нет, проверив MAC-адрес IPC. Если MAC-адреса источника нетегированных пакетов имеют тот же MAC-адрес, что и IPC. Эти пакеты определяются как видеофайлы и передаются в ВЛВС наблюдения. Если входящий видеопакет тегирован, и его VLAN ID равен VLAN наблюдения, приоритет пакета будет отмечен приоритетом видеотрафика.

Если IPC одновременно распознается по адресу OUI и протоколу ONVIF, этот IPC будет распознан протоколом ONVIF и предпримет соответствующие действия. Если ресурс, поддерживаемый устройством ONVIF, исчерпан, IPC будет распознан по адресу OUI.

Для использования этой команды необходимо, чтобы сеть VLAN, которая будет указана в качестве сети наблюдения, уже существовала.

Если сеть VLAN наблюдения настроена, сеть командой **vlan** не может быть удалена.

### Пример

В этом примере показано, как включить функцию VLAN наблюдения и настроить VLAN 1001 как Surveillance VLAN.

```
Switch# configure terminal
Switch(config)# surveillance vlan 1001
Switch(config)#
```

## 60-2 surveillance vlan aging

Данная команда используется для настройки времени устаревания (Aging Time) для устаревших динамических Member-портов Surveillance VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**surveillance vlan aging MINUTES**  
**no surveillance vlan aging**

#### Параметры

<i>MINUTES</i>	Укажите время устаревания Surveillance VLAN в диапазоне от 1 до 65535 минут.
----------------	--

#### По умолчанию

Значение по умолчанию – 720 минут.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте данную команду для настройки времени устаревания для устройства Surveillance и автоматически изученных Member-портов Surveillance VLAN.

Когда последнее устройство Surveillance, подключенное к порту, перестает отправлять трафик и MAC-адрес данного устройства устаревает, запускается таймер времени устаревания Surveillance VLAN. По истечении данного времени порт будет удален из Surveillance VLAN.

Если трафик Surveillance возобновляется в течение времени устаревания, таймер будет отменен.

#### Пример

В данном примере показано, как настроить время устаревания Surveillance VLAN на 30 минут.

```
Switch# configure terminal
Switch(config)#surveillance vlan aging 30
Switch(config)#
```

### 60-3 surveillance vlan enable

Данная команда используется для включения функции Surveillance VLAN на портах. Используйте форму **no**, чтобы отключить функцию Surveillance VLAN на портах.

**surveillance vlan enable**  
**no surveillance vlan enable**

#### Параметры

Нет

#### По умолчанию

По умолчанию данная функция отключена.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Команда доступна для настройки интерфейсов физического порта и port-channel. Команда используется на портах доступа и гибридных портах.

Для включения функции Surveillance VLAN необходимо применить команду **surveillance vlan** в режиме Global Configuration Mode и команду **surveillance vlan enable** в режиме Interface Configuration Mode.

При включении на порту Surveillance VLAN порт будет автоматически распознан как нетегированный член Surveillance VLAN. Полученные нетегированные пакеты Surveillance будут перенаправлены в Surveillance VLAN. При соответствии исходных MAC-адресов пакетов адресам уникального идентификатора организации (OUI), настроенным при помощи команды **surveillance vlan mac-address**, полученные пакеты распознаются как пакеты Surveillance.

**Пример**

В данном примере показано, как включить функцию Surveillance VLAN на физическом порту Ethernet 1/0/1.

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

**60-4 surveillance vlan mac-address**

Данная команда используется для добавления уникального идентификатора организации (OUI), определяемого с устройства системы видеонаблюдения в Surveillance VLAN. Используйте форму **no**, чтобы удалить OUI устройства Surveillance.

**surveillance vlan mac-address MAC-ADDRESS MASK [component-type {vms | vms-client | video-encoder | network-storage | other} description TEXT]**  
**no surveillance vlan mac-address MAC-ADDRESS MASK**

**Параметры**

<i>MAC-ADDRESS</i>	Укажите MAC-адрес OUI.
<i>MASK</i>	Укажите соответствующую битовую маску MAC-адреса OUI.
<b>component-type</b>	(Опционально) Укажите устройство системы видеонаблюдения, которое может быть автоматически обнаружено при помощи Surveillance VLAN.
<b>vms</b>	(Опционально) Укажите сервер VMS (Video Management Server – сервер для управления системой видеонаблюдения).
<b>vms-client</b>	(Опционально) Укажите клиента VMS в системе видеонаблюдения.
<b>video-encoder</b>	(Опционально) Укажите видеокодер в системе видеонаблюдения.
<b>network-storage</b>	(Опционально) Укажите сетевое хранилище в системе

	видеонаблюдения.
<b>other</b>	(Опционально) Укажите другие устройства в системе видеонаблюдения (IP Surveillance Devices).
<b>description TEXT</b>	(Опционально) Укажите описание OUI. Максимально допустимое количество символов – 32.

**По умолчанию**

OUI Address	Mask	Component Type	Description
28-10-7B-00-00-00	FF-FF-FF-E0-00-00	T-COM Device	IP Surveillance Device
Device 28-10-7B-20-00-00	FF-FF-FF-F0-00-00	T-COM Device	IP Surveillance Device
Device B0-C5-54-00-00-00	FF-FF-FF-80-00-00	T-COM Device	IP Surveillance Device
Device F0-7D-68-00-00-00	FF-FF-FF-F0-00-00	T-COM Device	IP Surveillance Device

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Используйте данную команду для добавления одного или нескольких OUI Surveillance VLAN. OUI используется для идентификации трафика видеонаблюдения с помощью функции Surveillance VLAN. Если MAC-адреса источника полученных пакетов соответствуют любому из шаблонов OUI, полученный пакет распознается как Surveillance.

OUI, полученный с устройства видеонаблюдения в Surveillance VLAN, не может совпадать с OUI по умолчанию.

OUI по умолчанию не может быть удален.

**Пример**

В данном примере показано, как добавить OUI для устройств Surveillance.

```
Switch# configure terminal
Switch(config)# surveillance vlan mac-address 00-01-02-03-00-00 FF-FF-FF-FF-00-00 component-
type vms description user1
Switch(config)#
```

**60-5 surveillance vlan onvif-discover-port**

Эта команда используется для настройки номера порта TCP/UDP для обнаружения потоков RTSP. Используйте **no** для возврата к настройкам по умолчанию.

```
surveillance vlan onvif-discover-port VALUE
no surveillance vlan onvif-discover-port
```

**Параметры**



<i>VALUE</i>	Введите здесь номер порта TCP/UDP. Диапазон может быть либо 554, либо от 1025 до 65535.
--------------	---

**По умолчанию**

По умолчанию это значение равно 554.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Эта команда используется для настройки номера порта TCP/UDP для обнаружения потоков RTSP. IPC с поддержкой ONVIF и NVR с поддержкой ONVIF используют WS-Discovery для поиска других устройств. После обнаружения IPC коммутатор может обнаружить NVR, прослушивая пакеты RTSP, HTTP и HTTPS между NVR и IPC. Эти пакеты нельзя прослушивать, если порт TCP/UDP не равен номеру порта RTSP.

**Пример**

В этом примере показано, как настроить номер порта TCP/UDP на 2000 для обнаружения потока RTSP.

```
Switch# configure terminal
Switch(config)# surveillance vlan onvif-discover-port 2000
Switch(config)#
```

**60-6 surveillance vlan onvif-ipc state**

Эта команда используется для настройки состояния IPC распознавания ONVIF. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

**surveillance vlan onvif-ipc *IP-ADDRESS* [*mac-address MAC-ADDRESS*] state {enable | disable}**  
**no surveillance vlan onvif-ipc *IP-ADDRESS* [*mac-address MAC-ADDRESS*] state**

**Параметры**

<i>IP-ADDRESS</i>	Введите здесь IP-адрес IPC.
<i>MAC-ADDRESS</i>	(Опционально) Введите MAC-адрес IPC, который распознается с помощью ONVIF.
<b>enable</b>	Указывает, что состояние ONVIF recognition IPC будет включено.
<b>disable</b>	Указывает, что состояние ONVIF recognition IPC будет отключено.

**По умолчанию**

По умолчанию эта функция включена.

**Режим ввода команды**

Global Configuration Mode

## Использование команды

Данная команда используется для настройки состояния IPC для распознавания ONVIF с указанием только IP-адреса IPC или IP- и MAC-адреса IPC. Когда IPC ONVIF распознан, можно настроить состояние для указанного устройства. Если имеется более одного IPC с одинаковым IP-адресом и MAC-адреса этих IPC не указаны, состояние этих IPC будет затронуто.

Эта функция используется для блокировки трафика IPC или нет. Если состояние IPC на порту отключено, трафик от IPC будет заблокирован.

### Пример

В этом примере показано, как включить режим IPC с IP-адресом 172.18.60.1.

```
Switch# configure terminal
Switch(config)# surveillance vlan onvif-ipc 172.18.60.1 state enable
Switch(config)#
```

## 60-7 surveillance vlan onvif-ipc description

Эта команда используется для настройки описания IPC, распознаваемого ONVIF. Используйте команду **no** для удаления описания.

**surveillance vlan onvif-ipc** *IP-ADDRESS* [*mac-address* *MAC-ADDRESS*] **description** *TEXT*  
**no surveillance vlan onvif-ipc** *IP-ADDRESS* [*mac-address* *MAC-ADDRESS*] **description**

### Параметры

<i>IP-ADDRESS</i>	Введите здесь IP-адрес IPC, признанного ONVIF.
<i>MAC-ADDRESS</i>	(Опционально) Введите MAC-адрес IPC, который распознается с помощью ONVIF.
<b>enable</b>	Введите здесь описание IPC, признанного ONVIF. Оно может содержать до 32 символов.

### По умолчанию

По умолчанию для IPC, признанного ONVIF, не определено описание.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Эта команда используется для настройки описания IPC, признанного ONVIF, с указанием только IP-адреса IPC или IP- и MAC-адреса IPC. Если имеется несколько IPC с одинаковым IP-адресом и MAC-адреса этих IPC не указаны, будет настроено описание этих IPC.

### Пример

В этом примере показано, как определить описание IPC с IP-адресом 172.18.60.1 как 'ipc1'.

```
Switch# configure terminal
Switch(config)# surveillance vlan onvif-ipc 172.18.60.1 description ipc1
Switch(config)#
```

## 60-8 surveillance vlan onvif-nvr description

Эта команда используется для настройки описания NVR с поддержкой ONVIF. Используйте команду **no** для удаления этого описания.

**surveillance vlan onvif-nvr** *IP-ADDRESS* [**mac-address** *MAC-ADDRESS*] **description** *TEXT*  
**no surveillance vlan onvif-nvr** *IP-ADDRESS* [**mac-address** *MAC-ADDRESS*] **description**

### Параметры

<i>IP-ADDRESS</i>	Введите здесь IP-адрес сетевого видеорегистратора с поддержкой ONVIF.
<i>MAC-ADDRESS</i>	(Опционально) Введите MAC-адрес сетевого видеорегистратора, который распознается с помощью ONVIF.
<b>enable</b>	Введите здесь описание сетевого видеорегистратора с поддержкой ONVIF. Он может содержать до 32 символов.

### По умолчанию

По умолчанию для NVR, признанного ONVIF, не определено описание.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Когда сетевой видеорегистратор ONVIF распознан, можно настроить описание для указанного устройства.

Эта команда используется для настройки описания распознанного ONVIF NVR с указанием только IP-адреса NVR или IP- и MAC-адреса NVR. Если существует несколько NVR с одинаковым IP-адресом, а MAC-адреса этих NVR не указаны, будет настроено описание этих NVR.

### Пример

В этом примере показано, как определить описание сетевого видеорегистратора с IP-адресом 172.18.60.2 как 'nvr1'.

```
Switch# configure terminal
Switch(config)# surveillance vlan onvif-nvr 172.18.60.2 description nvr1
Switch(config)#
```

## 60-9 surveillance vlan qos

Эта команда используется для настройки приоритета CoS для входящего трафика VLAN наблюдения. Используйте форму **no** этой команды для возврата к настройкам по умолчанию.

```
surveillance vlan qos COS-VALUE
no surveillance vlan qos
```

### Параметры

<i>COS-VALUE</i>	Указывает приоритет сети наблюдения VLAN. Доступное значение - от 0 до 7.
------------------	---

### По умолчанию

Значение по умолчанию 5.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Пакеты наблюдения, поступающие на порт с включенной ВЛВС наблюдения, помечаются COS, указанным командой.

Пометка COS позволяет отличить трафик VLAN наблюдения от трафика данных по качеству обслуживания.

### Пример

В этом примере показано, как настроить приоритет VLAN наблюдения на 7.

```
Switch# configure terminal
Switch(config)# surveillance vlan qos 7
Switch(config)#
```

## 60-10 show surveillance vlan

Эта команда используется для отображения конфигураций VLAN наблюдения.

```
show surveillance vlan [interface [INTERFACE-ID [, | -]]]
show surveillance vlan device [interface [INTERFACE-ID [, | -]]]
```

### Параметры

<b>device</b>	Указывает для отображения информации об изученных устройствах наблюдения.
<b>interface</b>	(Опционально) Указывает на отображение информации о VLAN наблюдения для портов.
<i>INTERFACE-ID</i>	(Опционально) Укажите порт, который будет отображаться.
,	(Опционально) Указывает серию интерфейсов или отделяет диапазон интерфейсов от предыдущего диапазона. До или после запятой пробел не допускается.
-	(Опционально) Указывает диапазон интерфейсов. До и после дефиса пробел не допускается.

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте эту команду для отображения конфигураций сети наблюдения VLAN.

Команда **show surveillance vlan** используется для отображения глобальных конфигураций сети наблюдения VLAN.

Команда **show surveillance vlan interface** используется для отображения конфигураций vlan наблюдения на интерфейсах.

Команда **show surveillance vlan device** используется для отображения устройства наблюдения, обнаруженного по его OUI.

**Пример**

В этом примере показано, как отобразить глобальные настройки сети наблюдения VLAN.

```
Switch# show surveillance vlan

Surveillance VLAN ID : 100
Surveillance VLAN CoS : 5
Aging Time           : 30 minutes
ONVIF Discover Port  : 554
Member Ports         :
Dynamic Member Ports :

Surveillance VLAN OUI :

OUI Address          Mask                Component Type      Description
-----
28-10-7B-00-00-00    FF-FF-FF-E0-00-00  D-Link Device      IP Surveillance Device
28-10-7B-20-00-00    FF-FF-FF-F0-00-00  D-Link Device      IP Surveillance Device
B0-C5-54-00-00-00    FF-FF-FF-80-00-00  D-Link Device      IP Surveillance Device
F0-7D-68-00-00-00    FF-FF-FF-F0-00-00  D-Link Device      IP Surveillance Device

Total OUI: 4

Switch#
```

**60-11 show surveillance vlan onvif-ipc interface**

Эта команда используется для отображения информации IPC на основе ONVIF.

**show surveillance vlan onvif-ipc interface [INTERFACE-ID [, | -]] {brief | detail}**

#### Параметры

<i>INTERFACE-ID</i>	(Опционально) Укажите порт, который будет отображаться.
,	(Опционально) Указывает серию интерфейсов или отделяет диапазон интерфейсов от предыдущего диапазона. До или после запятой пробел не допускается.
-	(Опционально) Указывает диапазон интерфейсов. До и после дефиса пробел не допускается.
<b>brief</b>	Указывает на отображение краткой информации об IP-камере на основе ONVIF.
<b>detail</b>	Указывает на отображение подробной информации об IP-камере на базе ONVIF.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Эта команда используется для отображения краткой или подробной информации IPC на основе ONVIF.

#### Пример

В этом примере показано, как отобразить краткую информацию об IP-камере на базе ONVIF.

```
Switch# show surveillance vlan onvif-ipc interface eth1/0/1 brief

Interface      : eth1/0/1
IP Address     : 10.90.90.1
MAC Address    : 00-01-02-03-04-05
Model         : P3384-VE
Manufacturer   : D-Link
Traffic       : Enabled
Throughput    : 5 Mbps
Description    : P3384-VE

Total Entries: 1

Switch#
```

В этом примере показано, как отобразить подробную информацию об IP-камере на базе ONVIF.

```
Switch# show surveillance vlan onvif-ipc interface ethernet 1/0/1 detail

Interface      : eth1/0/1
IP Address     : 10.90.90.1
MAC Address    : 00-01-02-03-04-05
Model         : P3384-VE
Manufacturer   : D-Link
State         : Enabled
Throughput    : 5 Mbps
Description    : P3384-VE
Protocol      : ONVIF
Power Consumption: 1.9W/15W
PoE           : 802.3af
PoE Status    : Enable

Total Entries: 1

Switch#
```

## 60-12 show surveillance vlan onvif-nvr interface

Эта команда используется для отображения информации о NVR и группах на базе ONVIF.

**show surveillance vlan onvif-nvr interface [INTERFACE-ID [, | -]] [ipc-list]**

### Параметры

<i>INTERFACE-ID</i>	(Опционально) Указывает порт для отображения.
,	(Опционально) Указывает серию интерфейсов или отделяет диапазон интерфейсов от предыдущего диапазона. До или после запятой пробел не допускается.
-	(Опционально) Указывает диапазон интерфейсов. До и после дефиса пробел не допускается.
<b>ipc-list</b>	(Опционально) Указывает для отображения информации о группе NVR.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Эта команда используется для отображения информации о NVR и группе на базе ONVIF. ID группы - это ID группы IPC, которые принадлежат группе NVR. NVR и управляемые им IPC должны иметь одинаковый идентификатор группы.

### Пример

В этом примере показано, как отобразить информацию о NVR на базе ONVIF.

```
Switch# show surveillance vlan onvif-nvr interface ethernet 1/0/1

Interface      : eth1/0/1
IP Address     : 111.111.111.111
MAC Address    : 00-03-02-03-04-08
IPC Number     : 2
Throughput    : 10 Mbps
Group         : Group 1
Description    : D-Link-NVR

Total Entries: 1

Switch#
```

В этом примере показано, как отобразить информацию о NVR на базе ONVIF, связанную с идентификатором группы 'ipc- list'.

```
Switch# show surveillance vlan onvif-nvr interface ethernet 1/0/1 ipc-list

Interface IP Address      MAC address      Group  Description
-----
1         10.90.90.90.1      00-01-02-03-04-05 1      D-Link-IPC-1
1         10.90.90.90.2      00-01-02-03-04-06 1      D-Link-IPC-2

Total Entries: 2

Switch#
```



## 61. Команды портов коммутатора

### 61-1 duplex

Эта команда используется для настройки duplex интерфейса физического порта. Используйте форму **no** для возврата к настройкам по умолчанию.

```
duplex {full | half | auto}
no duplex
```

#### Параметры

<b>full</b>	Укажите для работы порта в режиме полного дуплекса (Full-Duplex Mode).
<b>half</b>	Указывает, что порт работает в полудуплексном режиме.
<b>auto</b>	Укажите, чтобы режим дуплекса на порту был определен автосогласованием (Auto-Negotiation).

#### По умолчанию

Для интерфейсов 1000BASE-T режим duplex будет установлен как **auto**.

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

Для модулей 1000BASE-T, если скорость установлена на 1000, то дуплексный режим не может быть установлен на полудуплексный. Если дуплексный режим установлен на полудуплекс, то скорость не может быть установлена на 1000.

Автосогласование будет включено, если для параметра скорости установлено значение auto или для параметра дуплекса установлено значение auto. Если параметр скорости установлен на auto, а параметр дуплекса установлен на фиксированный режим, будет согласована только скорость. Объявленные возможности будут настроены на дуплексный режим в сочетании со всеми возможными скоростями. Если скорость установлена на фиксированную скорость, а дуплекс установлен на auto, согласовывается только режим дуплекса. Рекламируемые возможности будут включать в себя как полнодуплексный, так и полудуплексный режим в сочетании с настроенными скоростями.

#### Пример

В этом примере показано, как настроить порт 1 для работы на принудительной скорости 100 Мбит и указать, что дуплексный режим должен быть установлен на auto-negotiated.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# speed 100
Switch(config-if)# duplex auto
Switch(config-if)#
```

## 61-2 flowcontrol

Данная команда используется для настройки возможности управления потоком (Flow Control) на интерфейсе порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**flowcontrol {on | off}**  
**no flowcontrol**

### Параметры

<b>on</b>	Укажите, чтобы включить на порту отправку или обработку кадров PAUSE, поступающих из удаленных портов.
<b>off</b>	Укажите, чтобы отключить отправку или не получать кадры PAUSE.

### По умолчанию

По умолчанию данная функция отключена.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

С помощью данной команды можно настроить возможность управления потоком только в программном обеспечении коммутатора. Фактическая операция, выполняемая средствами аппаратного обеспечения, может отличаться от заданной, так как возможность управления потоком настраивается как на текущем, так и на удаленном порту/устройстве.

При установлении фиксированной скорости заданная настройка управления потоком будет окончательной. При установлении скорости, определенной автосогласованием, окончательная примененная настройка управления потоком будет основана на согласовании настроек локального устройства и коммутатора. В данном случае настройка управления потоком осуществляется с помощью локального устройства.

Данная команда не поддерживается коммутаторами, объединенными в физический стек.

### Пример

В данном примере показано, как включить управление потоком на интерфейсе Ethernet 1/0/1.

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

## 61-3 mdix

Данная команда используется для настройки состояния MDIX порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
mdix {auto | normal | cross}
no mdix
```

### Параметры

<b>auto</b>	Укажите, чтобы включить режим Auto-MDIX Mode.
<b>normal</b>	Укажите, чтобы включить режим Normal Mode.
<b>cross</b>	Укажите, чтобы включить режим Cross Mode.

### По умолчанию

Режим по умолчанию – Auto.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Данная команда неприменима на порту, к которому подключен оптоволоконный кабель.

### Пример

В данном примере показано, как настроить режим Auto-MDIX Mode на интерфейсе Ethernet 1/0/1.

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

## 61-4 speed

Данная команда используется для настройки скорости интерфейса физического порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
speed {10 | 100 | 1000 [master | slave] | 10giga [master | slave] | auto [SPEED-LIST]} [rj45 | sfp]
no speed [rj45 | sfp]
```

### Параметры

<b>10</b>	Укажите, чтобы установить скорость 10 Мбит/с.
<b>100</b>	Укажите, чтобы установить скорость 100 Мбит/с.
<b>1000</b>	Укажите, чтобы установить скорость 1000 Мбит/с на медных портах. Необходимо вручную задать статус порта: Master (основное

	устройство) или Slave (дополнительное устройство). Укажите, чтобы отключить автосогласование на всех оптических портах (1000Base-SX/LX).
<b>master   slave</b>	Укажите статус порта: Master (основное устройство) или Slave (дополнительное устройство). Данный параметр применим только к устройствам, подключенным к порту 1000Base-T.
<b>10giga</b>	Укажите, чтобы установить скорость 10 Гбит/с.
<b>master   slave</b>	Укажите статус порта: Master (основное устройство) или Slave (дополнительное устройство). Данный параметр применим только к устройствам, подключенным к порту 10GBase-T.
<b>auto</b>	Указывает, что для медных портов он определяет скорость и управление потоком через автосогласование с партнером по каналу. Указывает, что для оптоволоконных портов (1000BASE-SX/LX) включается опция автосогласования. Автосогласование начнет согласование тактовой частоты и управления потоком с партнером по каналу.
<b>SPEED-LIST</b>	(Опционально) Указывает список скоростей, с которыми коммутатор будет выполнять автосогласование. Скорость может быть <b>10</b> , <b>100</b> и/или <b>1000</b> . Используйте запятую (,) для разделения нескольких скоростей. Если список скоростей не указан, будут рекламироваться все скорости.

### По умолчанию

Скорость будет установлена как **auto** для интерфейсов 1000BASE-T.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Если указанная скорость не поддерживается оборудованием, будут возвращены сообщения об ошибках. Для соединения 1000BASE-T, если скорость указана 1000 Мбит/с, порт должен быть настроен как ведущий или ведомый.

Если скорость установлена на 1000 Мбит/с или 10 Гбит/с, то дуплексный режим не может быть установлен на полудуплекс. Если дуплексный режим установлен на полудуплекс, то скорость не может быть установлена на 1000 Мбит/с или 10 Гбит/с.

Автосогласование будет включено, если либо для параметра скорости установлено значение **auto**, либо для параметра duplex установлено значение **auto**. Если для параметра скорости установлено значение **auto**, а для параметра duplex установлен фиксированный режим. Будет согласована только скорость. Объявленные возможности будут настроены на duplex режим в сочетании со всеми возможными скоростями. Если скорость установлена на фиксированную скорость, а duplex установлен на **auto**, согласовывается только режим duplex. Рекламируемые возможности будут соответствовать как sub-duplex, так и sub-duplex режиму в сочетании с настроенными скоростями.

Для соединений 10GBASE-R, если включено автосогласование, система автоматически настроит скорость (1000M или 10G) в соответствии с типом SFP/SFP+.

## Пример

В данном примере показано, как на интерфейсе Ethernet 1/0/1 включить автосогласование, при котором будут использоваться только скорости 10 Мбит/с или 100 Мбит/с.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# speed auto 10,100
Switch(config-if)#
```

## 62. Команды управления системных файлов

### 62-1 boot config

Данная команда используется для указания конфигурационного файла, который будет использован при следующем запуске устройства.

**boot config {Config1 | Config2}**

#### Параметры

<b>Config1</b>	Указывает на использование Config1 в качестве файла начальной конфигурации.
<b>Config2</b>	Указывает на использование Config2 в качестве файла начальной конфигурации.

#### По умолчанию

По умолчанию используется Config1.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Команда используется для указания файла начальной конфигурации. Если действующий файл конфигурации отсутствует, устройство будет сконфигурировано в состояние по умолчанию.

#### Пример

В этом примере показано, как настроить файл "Config2" в качестве файла начальной конфигурации.

```
Switch#configure terminal
Switch(config)#boot config Config2
Switch(config)#
```

### 62-2 boot image

Данная команда используется для указания файла образа, который будет использован при следующем запуске устройства.

**boot image [check] {Image1 | Image2}**

#### Параметры

<b>check</b>	(Опционально) Указывает на отображение информации о микропрограмме для указанного файла. Эта информация включает номер версии и описание модели.
<b>Image1</b>	Указывает на использование Image1 в качестве файла

	загрузочного образа.
<b>Image2</b>	Указывает на использование Image2 в качестве файла загрузочного образа.

**По умолчанию**

По умолчанию загрузочным образом является **Image1**.

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

При использовании команды **boot image** указанный файл образа загрузки станет файлом образа начальной загрузки при следующей перезагрузке. Используйте эту команду, чтобы назначить файл в качестве файла образа следующей загрузки. Система проверит модель и контрольную сумму, чтобы определить, является ли файл действительным файлом образа.

Параметр **check** предназначен для проверки информации о файле, чтобы пользователь мог понять, подходит ли указанный файл для использования в качестве **загрузочного образа** или нет. Настройка команды загрузочного образа будет немедленно сохранена в NVRAM, которая представляет собой пространство, отделенное от начальной конфигурации.

**Пример**

В этом примере показано, как указать, что коммутатор должен использовать файл образа с именем "Image1" в качестве файла загрузочного образа при следующем запуске.

```
Switch#configure terminal
Switch(config)#boot image Image1
Switch(config)#
```

**62-3 clear running-config**

Данная команда используется для удаления текущей конфигурации системы (running configuration).

**clear running-config****Параметры**

Нет

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Используйте данную команду, чтобы удалить конфигурацию системы, сохраненную в DRAM-память. Данные конфигурации вернутся к настройкам по умолчанию. Перед использованием данной команды сохраните резервную копию конфигурации с помощью команды **copy** или выгрузите профиль конфигурации на TFTP-сервер.

При удалении настроек конфигурации системы информация о стеке не удаляется, однако, стираются параметры IP. Таким образом, все существующие удаленные подключения будут прерваны. После применения данной команды необходимо настроить IP-адрес через локальную консоль.

### Пример

В данном примере показано, как удалить текущую конфигурацию системы.

```
Switch#clear running-config

This command will clear the system's configuration to the factory
default settings, including the IP address.
Clear running configuration? (y/n) [n] y

Switch#
```

## 62-4 reset system

Данная команда используется для сброса системы и удаления ранее сохраненной конфигурации с дальнейшей перезагрузкой коммутатора.

### reset system

#### Параметры

Нет

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Используйте данную команду для удаления конфигурации системы, включая информацию о стеке. Данные конфигурации вернутся к настройкам по умолчанию, будет создан соответствующий конфигурационный файл загрузки, затем будет выполнен перезапуск коммутатора. Перед использованием данной команды сохраните резервную копию конфигурации с помощью команды **copy** или выгрузите профиль конфигурации на TFTP-сервер.

### Пример

В данном примере показано, как сбросить систему и вернуться к настройкам по умолчанию.



```
Switch# reset system
```

```
This command will clear all of system configuration as factory
default setting including IP parameters and stacking information.
Clear system configuration, save, reboot? (y/n) [n] y
```

```
Saving configurations and logs to NV-RAM..... Done.
Please wait, the switch is rebooting...
```

## 62-5 configure replace

Данная команда используется для замены текущей конфигурации указанным конфигурационным файлом.

**configure replace** **{tftp: //location/filename | flash: FILENAME}** **[force]**

### Параметры

<b>tftp:</b>	Укажите конфигурационный файл с TFTP-сервера.
<i>//location/filename</i>	Укажите URL конфигурационного файла на TFTP-сервере.
<b>flash:</b>	Укажите, что конфигурационный файл из NVRAM.
<i>FILENAME</i>	Укажите имя конфигурационного файла, хранящегося в NVRAM.
<b>force</b>	(Опционально) Укажите, чтобы принудительно применить команду без дополнительного подтверждения.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте данную команду, чтобы заменить текущую конфигурацию указанным конфигурационным файлом. Текущая конфигурация будет удалена перед применением указанной конфигурации.



**Примечание:** при выполнении данной команды текущая конфигурация полностью меняется на конфигурацию указанного файла. В указанном конфигурационном файле должна быть представлена полная конфигурация, а не частичная.

Перед использованием данной команды сохраните резервную копию конфигурации с помощью команды **copy** или выгрузите профиль конфигурации на TFTP-сервер.

### Пример

В этом примере показано, как загрузить файл "config.cfg" с сервера TFTP и заменить им текущую работающую конфигурацию.

```
Switch# configure replace tftp: //10.0.0.66/config.cfg

This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. [y/n]: y

Accessing tftp://10.0.0.66/config.cfg...
Transmission start...
Transmission finished, file length 45422 bytes.
Executing script file config.cfg .....
Executing done

Switch#
```

В данном примере показано, как заменить текущую текущую конфигурацию на файл "Config1", хранящийся в NVRAM устройства. Выполните команду немедленно без подтверждения.

```
Switch#configure replace flash: Config1 force

Executing script file Config1 .....
Executing done

Switch#
```

## 62-6 copy

Данная команда используется для копирования файлов.

```
copy SOURCE-URL DESTINATION-URL
copy SOURCE-URL {tftp: [//LOCATION/DESTINATION-URL]}
copy {tftp: [//LOCATION/SOURCE-URL]} DESTINATION-URL
```

### Параметры

<i>SOURCE-URL</i>	Укажите URL источника исходного файла, который необходимо скопировать. Особые формы URL представлены следующими ключевыми словами: Укажите <b>startup-config</b> в качестве URL источника, чтобы выгрузить конфигурацию, которая будет применена после
-------------------	---

	<p>запуска коммутатора, сохранить ее как файл в файловой системе или использовать в качестве текущей конфигурации.</p> <p>Укажите <b>running-config</b> в качестве URL источника, чтобы выгрузить текущую конфигурацию, сохранить ее в качестве загрузочной конфигурации или как файл в файловой системе.</p> <p>Укажите <b>flash: [PATH-FILE-NAME]</b> в качестве URL источника, чтобы скопировать исходный файл в файловую систему.</p> <p>Укажите <b>log</b> в качестве URL, чтобы выгрузить системный журнал на TFTP-сервер или сохранить его как файл в файловую систему.</p> <p>Укажите <b>attack-log UNIT-ID</b> в качестве URL источника, чтобы выгрузить журнал атак указанного Unit.</p>
<b>DESTINATION-URL</b>	<p>Укажите URL назначения скопированного файла. Особые формы URL представлены следующими ключевыми словами:</p> <p>Укажите <b>running-config</b> в качестве URL назначения, чтобы применить конфигурацию к текущей конфигурации.</p> <p>Укажите <b>startup-config</b> в качестве URL назначения, чтобы сохранить конфигурацию, которую необходимо применить при следующем запуске. Текущая конфигурация будет сохранена в NVRAM, а имя файла будет совпадать с именем файла, указанным при использовании команды <b>bootconfig</b>.</p> <p>Укажите <b>flash: [PATH-FILE-NAME]</b> в качестве URL назначения, чтобы указать имя копируемого файла в файловой системе. При указании относительного пути файл будет загружен на все устройства в стеке и сохранен в текущем пути каждого Unit. При указании абсолютного пути файл будет загружен в место, которое было задано абсолютным путем. При отсутствии информации об Unit в абсолютном пути будет назначен основное устройство (Master).</p>
<b>LOCATION</b>	(Опционально) Указывает IPv4/IPv6 адрес сервера TFTP.

**По умолчанию**

Нет

**Режим ввода команды****Использование команды**

Используйте данную команду для копирования файлов в файловую систему, загрузки/выгрузки конфигурационного файла или файла образа, загрузки системного журнала на TFTP-сервер. Чтобы выгрузить текущую конфигурацию или сохранить ее в качестве загрузочной конфигурации, укажите **running-config** в качестве URL источника. Чтобы сохранить текущую конфигурацию в качестве загрузочной конфигурации, укажите **startup-config** в качестве URL назначения.

Если в качестве назначения указана загрузочная конфигурация, файл источника будет скопирован в файл, указанный в команде **boot config**. Исходный файл загрузочной конфигурации будет перезаписан.

Чтобы применить необходимый конфигурационный файл к текущей конфигурации, при использовании команды **copy** укажите **running-config** в качестве URL назначения. Данный конфигурационный файл будет сразу же применен, используя метод Increment. Указанная конфигурация будет объединена с текущей конфигурацией. Текущая конфигурация будет удалена только после применения указанной конфигурации.

Если в качестве источника указан системный журнал, а в качестве назначения указан URL, текущий системный журнал будет скопирован на указанный URL.

Чтобы отобразить файл на удаленном TFTP-сервере, необходимо использовать URL с префиксом «tftp://».

Чтобы загрузить образ программного обеспечения, используйте команду **copy tftp://** для загрузки файла с TFTP-сервера в файловую систему. Чтобы указать данный файл в качестве файла образа для загрузки, используйте команду **boot image**.

### Пример

В этом примере показано, как настроить рабочую конфигурацию коммутатора методом инкремента с использованием конфигурации под названием "switch-config.cfg", загруженной с TFTP-сервера 10.1.1.254.

```
Switch#copy tftp: //10.1.1.254/switch-config.cfg running-config

Address of remote host [10.1.1.254]?
Source filename [switch-config.cfg]?
Destination filename running-config? [y/n]: y

Accessing tftp://10.1.1.254/switch-config.cfg...
Transmission start...
Transmission finished, file length 29974 bytes.
Executing script file switch-config.cfg .....
Executing done

Switch#
```

В данном примере показано, как выгрузить текущую конфигурацию на TFTP-сервер для хранения.

```
Switch#copy running-config tftp: //10.1.1.254/switch-config.cfg

Address of remote host [10.1.1.254]?
Destination filename [switch-config.cfg]?
Accessing tftp://10.5.2.101/switch-config.cfg...
Transmission start...
Transmission finished, file length 28999 bytes.

Switch#
```

В данном примере показано, как сохранить текущую конфигурацию во FLASH-память и использовать ее при следующем запуске устройства.

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

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

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

Switch#
```

В этом примере показано, как выполнить файл "Config2" в NVRAM немедленно, используя метод инкремента.

```
Switch#copy flash: Config2 running-config

Source filename [Config2]?
Destination filename running-config? [y/n]: y

Executing script file Config2 .....
Executing done

Switch#
```

В этом примере показано, как загрузить файл изображения с сервера TFTP.

```
Switch#copy tftp: //10.1.1.254/runtime.had flash: Image1

Address of remote host [10.1.1.254]?
Source filename [runtime.had]?
Accessing tftp://10.1.1.254/runtime.had...
Transmission start...
Transmission finished, file length 8713712 bytes.
Please wait, programming flash..... 100 %
Please wait, programming flash for language files .....Done.

Switch#
```

## 62-7 show boot

Данная команда используется для отображения настроек конфигурационного файла и загрузочного образа.

**show boot**

**Параметры**

Нет

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Команда используется для отображения настроек конфигурационного файла и загрузочного образа.

**Пример**

В данном примере показано, как отобразить информацию о загрузке системы.

```
Switch#show boot

Unit 1
  Boot image: /c:/Image1
  Boot config: /c:/Config1

Switch#
```

**62-8 show running-config**

Данная команда используется для отображения команд текущего конфигурационного файла.

**show running-config [effective | all] [interface *INTERFACE-ID* | vlan *VLAN-ID*]**

**Параметры**

<b>effective</b>	(Опционально) Указывает на отображение конфигураций команд, которые влияют на поведение коммутатора. Например, если STP была отключена, будет отображена только команда <b>disable stp</b> . Все остальные настройки нижнего уровня относительно STP отображаться не будут. Настройки нижнего уровня будут отображаться только в том случае, если настройки верхнего уровня включены. Если этот параметр не выбран, будут отображаться только измененные конфигурации, отличные от конфигурации по умолчанию.
<b>all</b>	(Опционально) Указывает на отображение всех конфигураций команд; включая команды, соответствующие параметрам по умолчанию. Если этот параметр не выбран, будут отображаться только измененные конфигурации, отличающиеся от конфигурации по умолчанию.
<b>interface <i>INTERFACE-ID</i></b>	(Опционально) Укажите интерфейс, который будет отображаться.
<b>vlan <i>VLAN-ID</i></b>	(Опционально) Укажите VLAN для отображения.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте эту команду для отображения текущей конфигурации работающей системы.

### Пример

В данном примере показано, как отобразить содержимое текущего конфигурационного файла.

```
Switch#show running-config
Building configuration...

Current configuration : 3092 bytes

!-----
!                   DGS-1250-28XMP Gigabit Ethernet Smart Managed Switch
!                   Configuration
!
!                   Firmware: Build 2.01.001
!                   Copyright (C) 2020 D-Link Corporation. All rights reserved.
!-----

environment temperature threshold thermal high 100 low 20
!
ip http timeout-policy idle 36000
!
line console
  session-timeout 0
!
line telnet
!
line ssh
!
debug enable
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

### 62-9 show startup-config

Данная команда используется для отображения содержимого конфигурационного загрузочного файла.

**show startup-config**

## Параметры

Нет

## По умолчанию

Нет

## Режим ввода команды

EXEC Mode

## Использование команды

Команда используется для отображения настроек конфигурации, с помощью которых система будет инициализирована.

## Пример

В этом примере показано, как отобразить содержимое файла конфигурации начальной загрузки.

```
Switch#show startup-config

!-----
!
!           DGS-1250-28XMP Gigabit Ethernet Smart Managed Switch
!
!                   Configuration
!
!
!                   Firmware: Build 2.01.001
!
!           Copyright(C) 2020 D-Link Corporation. All rights reserved.
!-----

# AAA START
# AAA END
!
# COMMAND LEVEL START
# COMMAND LEVEL END
# LEVEL START
# LEVEL END
# ACCOUNT START
# ACCOUNT END
!
ip http timeout-policy idle 36000
ignore wizard
!
line console
  session-timeout 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```



## 63. Команды System Log

### 63-1 clear logging

Данная команда используется для удаления сообщений логирования из буфера системного логирования.

**clear logging**

#### Параметры

Нет

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Команда позволяет удалить все записи логирования из буфера системного логирования.

#### Пример

В данном примере показано, как удалить все записи логирования из буфера системного логирования.

```
Switch# clear logging
Clear logging? (y/n) [n] y
Switch#
```

### 63-2 logging buffered

Данная команда используется для включения логирования системных сообщений в локальный буфер сообщений. При использовании формы **no** команда отключит логирование системных сообщений в локальный буфер сообщений. Используйте команду **default logging buffered**, чтобы вернуть настройки по умолчанию.

**logging buffered [severity {SEVERITY-LEVEL | SEVERITY-NAME}] [discriminator NAME][write-delay {SECONDS | infinite}]**  
**no logging buffered default logging buffered**

#### Параметры

---

*SEVERITY-LEVEL*

(Опционально) Укажите уровень важности системных сообщений. Сообщения на этом уровне важности или более серьезном уровне будут логироваться в буфер сообщений. Значение может быть от 0 до 7, где 0 –

---

	наиболее важный уровень. Коды уровней важности: emergencies (чрезвычайные) – система не работоспособна (0), alerts (предупреждения) – система требует немедленного вмешательства (1), critical – состояние системы критическое (2), errors – сообщения об ошибках (3), warnings – предупреждения о возможных проблемах (4), notifications – уведомления о нормальных, но важных событиях (5), informational – информационные сообщения (6), debugging – отладочные сообщения (7). Если значение не указано, значение уровня по умолчанию – warnings (4).
<i>SEVERITY-NAME</i>	(Опционально) Укажите название уровня важности системных сообщений. Имена уровней важности: <b>emergencies (0), alerts (1), critical (2), errors (3), warnings (4), notifications (5), informational (6), debugging (7)</b> .
<b>discriminator</b>	(Опционально) Укажите discriminator для фильтрации сообщений, отправляемых в локальный буфер.
<b>write-delay SECONDS</b>	(Опционально) Укажите задержку периодической записи буфера логирования во FLASH-память на указанное количество секунд.

**По умолчанию**

По умолчанию используется уровень важности warning (4).

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Системные сообщения можно логировать в локальный буфер сообщений, локальную консоль или в другие места. Сообщения должны быть введены в локальный буфер сообщений перед отправкой в другие точки назначения.

Команда не будет применена, если указанный discriminator не существует. В таком случае будут применяться настройки по умолчанию.

Укажите уровень важности сообщений для ограничения системных сообщений, логируемых в буфер (это позволит уменьшить число логированных сообщений). Сообщения указанного уровня или выше будут логироваться в буфер. Если буфер будет заполнен, старые записи будут удалены, чтобы освободить место, необходимое для новых сообщений.

Содержимое буфера сообщений периодически будет сохраняться во FLASH-память, чтобы сообщения можно было восстановить при перезагрузке. Интервал сохранения записей из буфера во FLASH-память можно указать. Содержимое сообщений логирования во FLASH будет перезагружено в буфер логирования при перезагрузке.

**Пример**

В данном примере показано, как включить логирование сообщений в буфер логирования и ограничить логирование сообщений с уровнем важности errors или выше.

```
Switch# configure terminal
Switch(config)# logging buffered severity errors
Switch(config)#
```

### 63-3 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

<i>NAME</i>	Укажите имя discriminator.
<b>facility</b>	(Опционально) Укажите подфильтр согласно настройке facility.
<i>STRING</i>	Укажите одно или более имен facility. Если используется несколько имен, они должны быть разделены запятой, без пробелов до и после запятой.
<b>includes</b>	Укажите для включения совпадающих сообщений. Несовпадающие сообщения будут фильтроваться.
<b>drops</b>	Укажите для фильтрации совпадающих сообщений.
<b>severity</b>	(Опционально) Укажите подфильтр на основе совпадений с уровнем важности.
<i>SEVERITY-LIST</i>	Укажите список уровней важности для фильтрации или включения.

#### По умолчанию

Нет

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Настройка существующего параметра discriminator. При вводе команды более ранние настройки будут переписаны на новые. Ассоциируйте discriminator с командами logging buffered и logging server.

#### Пример

В данном примере показано, как создать discriminator с именем «buffer-filter», указывающим два подфильтра, один на основе уровня важности, а другой на основе facility.

```
Switch# configure terminal
Switch(config)# logging discriminator buffer-filter facility includes STP severity includes 1-4,6
Switch(config)#
```

## 63-4 logging server

Данная команда используется для создания серверного узла SYSLOG для логирования системных сообщений или вывода при отладке. При использовании формы **no** команда удалит серверный узел SYSLOG.

**logging server** {*IP-ADDRESS* | *IPV6-ADDRESS*} [**severity** {*SEVERITY-LEVEL* | *SEVERITY-NAME*}] [**facility** {*FACILITY-NUM* | *FACILITY-NAME*}] [**discriminator** *NAME*] [**port** *UDP-PORT*]  
**no logging server** {*IP-ADDRESS* | *IPV6-ADDRESS*}

### Параметры

<i>IP-ADDRESS</i>	Укажите IP-адрес серверного узла SYSLOG.
<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес серверного узла логирования.
<i>SEVERITY-LEVEL</i>	(Опционально) Укажите уровень важности системных сообщений. Сообщения на этом уровне важности или более серьезном уровне будут логироваться в буфер сообщений. Значение может быть от 0 до 7, где 0 – наиболее важный уровень. Коды уровней важности: emergencies (чрезвычайные) – система не работоспособна ( <b>0</b> ), alerts (предупреждения) – система требует немедленного вмешательства ( <b>1</b> ), critical – состояние системы критическое ( <b>2</b> ), errors – сообщения об ошибках ( <b>3</b> ), warnings – предупреждения о возможных проблемах ( <b>4</b> ), notifications – уведомления о нормальных, но важных событиях ( <b>5</b> ), informational – информационные сообщения ( <b>6</b> ), debugging – отладочные сообщения ( <b>7</b> ). Если значение не указано, значение уровня по умолчанию – warnings ( <b>4</b> ).
<i>SEVERITY-NAME</i>	(Опционально) Укажите название уровня важности системных сообщений. Имена уровней важности: <b>emergencies</b> (0), <b>alerts</b> (1), <b>critical</b> (2), <b>errors</b> (3), <b>warnings</b> (4), <b>notifications</b> (5), <b>informational</b> (6), <b>debugging</b> (7).
<i>FACILITY-NUM</i>	(Опционально) Укажите десятичное значение от 0 до 23 для facility. Если значение не указано, по умолчанию будет использоваться local7 ( <b>23</b> ). Для более подробной информации обратитесь к параграфу <b>Использование команды</b> .
<i>FACILITY-NAME</i>	(Опционально) Укажите имя для facility. Если значение не указано, по умолчанию будет использоваться <b>local7</b> (23). Для более подробной информации обратитесь к параграфу <b>Использование команды</b> .
<b>discriminator</b> <i>NAME</i>	(Опционально) Укажите для фильтрации сообщений на сервер логирования согласно настройке discriminator.
<b>port</b> <i>UDP-PORT</i>	(Опционально) Укажите номер порта UDP, который будет использоваться сервером SYSLOG. Доступен диапазон значений от 1024 до 65535, а также 514 (распространенный порт IANA). Если значение не указано, номер UDP-порта по умолчанию – 514.

### По умолчанию

Нет

**Режим ввода команды**

Global Configuration Mode

**Использование команды**

Системные сообщения можно логировать в локальный буфер сообщений, локальную консоль или на удаленные узлы. Сообщения должны быть введены в локальный буфер сообщений перед отправкой на сервер логирования.

Ниже представлена таблица значений Facility.

Номер Facility	Имя Facility	Описание
0	kern	Сообщения ядра
1	user	Сообщения уровня пользователя
2	mail	Система почты
3	daemon	Системные daemon
4	auth1	Сообщения системы безопасности/авторизации
5	syslog	Сообщения, генерируемые SYSLOG
6	lpr	Подсистема Line Printer
7	news	Подсистема сетевых новостей
8	uucp	Подсистема UUCP
9	clock1	Clock daemon
10	auth2	Сообщения системы безопасности/авторизации
11	ftp	FTP daemon
12	ntp	Подсистема NTP
13	logaudit	Аудит логирования
14	logalert	Предупреждение логирования
15	clock2	Clock daemon (note 2)
16	local0	Локальное использование 0 (local0)
17	local1	Локальное использование 1 (local1)
18	local2	Локальное использование 2 (local2)
19	local3	Локальное использование 3 (local3)
20	local4	Локальное использование 4 (local4)
21	local5	Локальное использование 5 (local5)
22	local6	Локальное использование 6 (local6)
23	local7	Локальное использование 7 (local7)

**Пример**

В данном примере показано, как включить логирование системных сообщений с уровнем важности выше warnings на удаленном узле 20.3.3.3.

```
Switch# configure terminal
Switch(config)# logging server 20.3.3.3 severity warnings
Switch(config)#
```

## 63-5 show logging

Данная команда используется для просмотра системных сообщений, логированных в локальном буфере.

**show logging [all | [REF-SEQ] [+ NN | - NN]]**

### Параметры

<b>all</b>	(Опционально) Укажите для отображения всех записей лога, начиная с последних.
<b>REF-SEQ</b>	(Опционально) Укажите для отображения с номера, следующего за указанным.
<b>+ NN</b>	(Опционально) Укажите количество сообщений, появившихся после указанного номера, следующим за указанным. Если значение не указано, отображение начинается от самых давних сообщений в буфере.
<b>- NN</b>	(Опционально) Укажите количество сообщений, появившихся до указанного номера, следующим за указанным. Если значение не указано, отображение начинается от самых последних сообщений в буфере.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Команда используется для просмотра системных сообщений, логированных в локальном буфере.

Каждое логированное в буфер сообщение ассоциировано с номером последовательности. При логировании сообщения назначается номер последовательности, начиная с 1. Номер последовательности вернется к 1 после достижения 100000.

Если пользователь указывает отображение количества сообщений после номера, следующим за указанным, более поздние сообщения будут отображаться до новых. Если пользователь указывает отображение количества сообщений с номера, следующим за указанным, новые сообщения будут отображаться до более поздних.

Если команда введена без опций, будет отображено 200 записей, начиная от самых последних.

### Пример

В данном примере показано, как отобразить сообщения в локальном буфере сообщений.

```
Switch# show
Switch# show logging

Total number of buffered messages: 2
#2 2015-03-25 16:37:36 Unit 1, Successful login through Console (Username: Anonymous)
#1 2015-03-25 16:35:54 INFO(6) Port eth1/0/1 link up, 1000Mbps FULL duplex

Switch#
```

## 63-6 show attack-logging

Данная команда используется для просмотра логированных сообщений об атаках.

**show attack-logging [index INDEX]**

### Параметры

<b>index INDEX</b>	(Опционально) Указывает список номеров индексов записей, которые необходимо отобразить. Если индекс не указан, будут отображены все записи в БД журнала атак.
--------------------	---

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Используйте эту команду для отображения сообщений журнала атак. Сообщения журнала атак относятся к сообщениям журнала, управляемым такими модулями, как DOS и модуль port-security. Этот тип сообщений журнала может генерировать большое количество сообщений и быстро привести к тому, что в системе закончится память системного журнала. Поэтому для этого типа сообщений в системном журнале можно хранить только первое сообщение, которое генерируется каждую минуту, а остальные сообщения хранить в отдельной таблице под названием журнал атак.

### Пример

В данном примере показано, как отобразить первую запись журнала атак.

```
Switch#show attack-logging

Attack log messages (total number:0)

Switch#
```

## 63-7 clear attack-logging

Данная команда используется для удаления сообщений об атаках.

## **clear attack-logging**

### **Параметры**

Нет

### **По умолчанию**

Нет

### **Режим ввода команды**

EXEC Mode

### **Использование команды**

Данная команда используется для удаления сообщений об атаках.

### **Пример**

В данном примере показано, как удалить все логированные сообщения об атаках.

```
Switch# clear attack-logging all  
Switch#
```



## 64. Команды времени и SNTP

### 64-1 clock set

Данная команда используется для установки системного времени вручную.

**clock set** *HH:MM:SS DAY MONTH YEAR*

#### Параметры

<i>HH:MM:SS</i>	Укажите текущее время: часы (24-часовой формат), минуты и секунды.
<i>DAY</i>	Укажите текущий день месяца.
<i>MONTH</i>	Укажите текущий месяц (January, Jan, February, Feb и т. д.).
<i>YEAR</i>	Укажите текущий год без сокращений.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Если система синхронизируется с помощью любого действующего внешнего механизма синхронизации, такого как SNTP, необходимо установить системное время. Используйте данную команду, если другие источники времени недоступны. Время, указанное в данной команде, принадлежит к часовому поясу, заданному конфигурацией команды **clock timezone**. Если устройство поддерживает функцию RTC (часы реального времени), время синхронизируется с RTC. Настроенные часы не будут сохранены в файле конфигурации.

Сервер SNTP является основным источником времени: даже если системное время было настроено вручную, при подключении к серверу SNTP время будет синхронизировано с его показателями.

#### Пример

В этом примере показано, как вручную установить программные часы на 18:00 4 июля 2020 года.

```
Switch# clock set 18:00:00 4 jul 2020
Switch#
```

### 64-2 clock summer-time

Данная команда используется для настройки автоматического перехода на летнее время. Используйте форму **no**, чтобы отключить автоматический переход на летнее время.

**clock summer-time recurring** *WEEK DAY MONTH HH:MM WEEK DAY MONTH HH:MM[OFFSET]*

**clock summer-time date** DATE MONTH YEAR HH:MM DATE MONTH YEAR HH:MM [OFFSET]  
**no clock summer-time**

### Параметры

<b>recurring</b>	Укажите дату начала и окончания летнего времени (день недели и месяц).
<b>date</b>	Укажите точную дату начала и окончания летнего времени.
<b>WEEK</b>	Укажите номер недели месяца (от 1 до 4) или слово «last», с помощью которого будет указана последняя неделя месяца.
<b>DAY</b>	Укажите день недели (sun, mon и т. д.).
<b>DATE</b>	Укажите день месяца (от 1 до 31).
<b>MONTH</b>	Укажите порядковый номер месяца в диапазоне от 1 до 12, где 1 – это январь, 2 – февраль и т. д.
<b>YEAR</b>	Укажите года, чтобы задать необходимый интервал для применения перехода на летнее время.
<b>HH:MM</b>	Укажите время (24-часовой формат) в часах и минутах.
<b>OFFSET</b>	(Опционально) Укажите количество минут, которое нужно добавить при переходе на летнее время. Значение по умолчанию – 60. Доступный диапазон смещения – 30, 60, 90 и 120 минут.

### По умолчанию

По умолчанию данная функция отключена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду, чтобы перейти на летнее время автоматически. У команды две формы: первая – повторяющаяся (**recurring**), которая используется для указания даты начала и окончания летнего времени (день недели и месяц); вторая – форма даты (**date**), которая используется для указания определенного числа месяца.

Первая часть данных команд указывает на начало летнего времени, а вторая – на конец.

### Пример

В этом примере показано, как указать, что летнее время начинается в первое воскресенье июня в 2 часа ночи и заканчивается в последнее воскресенье октября в 2 часа ночи.

```
Switch# configure terminal
Switch(config)# clock summer-time recurring 1 sun jun 2:00 last sun oct 2:00
Switch(config)#
```

## 64-3 clock timezone

Данная команда используется для настройки и отображения часового пояса. Используйте форму **no**, чтобы настроить время в формате UTC (всемирное координированное время).

**clock timezone {+ | -} HOURS-OFFSET [MINUTES-OFFSET]**  
**no clock timezone**

#### Параметры

+	Укажите количество часов, которых необходимо прибавить к UTC.
-	Укажите количество часов, которых необходимо вычесть из UTC.
<i>HOURS-OFFSET</i>	Укажите разницу во времени с UTC в часах.
<i>MINUTES-OFFSET</i>	(Опционально) Укажите разницу во времени с UTC в минутах.

#### По умолчанию

Часовой пояс по умолчанию – UTC.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Время, полученное с сервера SNTP, синхронизируется с форматом UTC. При настройке местного времени учитывается формат UTC, часовой пояс и настройки перехода на летнее время.

#### Пример

В данном примере показано, как настроить часовой пояс PST (Североамериканское Тихоокеанское Стандартное Время), который на 8 часов опережает время UTC.

```
Switch# configure terminal
Switch(config)# clock timezone - 8
Switch(config)#
```

## 64-4 show clock

Данная команда используется для отображения информации о времени и дате.

**show clock**

#### Параметры

Нет

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

### Использование команды

Также данная команда используется для отображения источника времени. Возможные источники: «No Time Source» (источник времени отсутствует) или «SNTP».

### Пример

В данном примере показано, как отобразить текущее время.

```
Switch#show clock

Current Time Source   : System Clock
Current Time         : 05:56:45, 2000-01-30
Time Zone            : UTC +00:00
Daylight Saving Time : Disabled

Switch#
```

## 64-5 show sntp

Данная команда используется для отображения информации о сервере SNTP.

**show sntp**

### Параметры

Нет

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Данная команда используется для отображения информации о сервере SNTP.

### Пример

В данном примере показано, как отобразить информацию об SNTP.

```

Switch#show sntp

SNTP Status           : Enabled
SNTP Poll Interval    : 720 sec

SNTP Server Status:

SNTP Server           Version Last Receive
-----
10.0.0.11             4          00:02:02
10::2                 -----
FE80::1111%vlan1     -----
-----

Total Entries:3

Switch#

```

## 64-6 sntp server

Данная команда используется для синхронизации системного времени с сервером SNTP. Используйте форму **no**, чтобы удалить сервер из списка серверов SNTP.

```

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

```

### Параметры

<i>IP-ADDRESS</i>	Укажите IP-адрес сервера, который обеспечивает синхронизацию времени.
<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес сервера времени.

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

SNTP – это упрощенная клиентская версия NTP. В отличие от NTP, SNTP может получать время только от серверов NTP; его нельзя использовать для предоставления времени другим системам. SNTP обеспечивает время с погрешностью 100 миллисекунд от точного времени, но, в отличие от NTP, не предоставляет сложные механизмы фильтрации и статистической обработки. Кроме того, SNTP не проверяет подлинность трафика, хотя с помощью настройки расширенного списка доступа можно обеспечить определённую степень защиты.

Введите данную команду один раз для каждого сервера NTP. Настроить систему и включить SNTP можно также с помощью команды **sntp broadcast client global configuration**. Чтобы создать несколько серверов SNTP, введите данную команду несколько раз, используя разные IP-адреса серверов SNTP.

Используйте форму **no**, чтобы удалить запись сервера SNTP. При удалении записи укажите точную информацию, введенную при первом подключении. Время, полученное с сервера SNTP, синхронизируется с форматом UTC.

### Пример

В данном примере показано, как синхронизировать системное время с сервером SNTP с IP-адресом 192.168.22.44.

```
Switch# configure terminal
Switch(config)# sntp server 192.168.22.44
Switch(config)#
```

## 64-7 sntp enable

Данная команда используется для включения функции SNTP. Используйте форму **no**, чтобы отключить функцию SNTP.

**sntp enable**  
**no sntp enable**

### Параметры

Нет

### По умолчанию

По умолчанию данная функция отключена.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Данная команда используется для включения/отключения функции SNTP.

### Пример

В данном примере показано, как включить функцию SNTP.

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

## 64-8 sntp interval

Данная команда используется для настройки интервала синхронизации часов SNTP-клиента с сервером. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**sntp interval SECONDS**  
**no sntp interval**

#### Параметры

---

<i>SECONDS</i>	Укажите интервал синхронизации в диапазоне от 30 до 99999 секунд.
----------------	---

---

#### По умолчанию

Значение по умолчанию – 720 секунд.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Данная команда используется для настройки интервала опроса (Polling Interval).

#### Пример

В данном примере показано, как настроить интервал на 100 секунд.

```
Switch# configure terminal
Switch(config)# sntp interval 100
Switch(config)#
```

## 65. Команды временного диапазона

### 65-1 periodic

Данная команда используется в режиме Time-Range Configuration Mode для указания профиля диапазона времени. Используйте форму **no**, чтобы удалить указанный временной диапазон.

**periodic {daily HH:MM to HH:MM | weekly WEEKLY-DAY HH:MM to [WEEKLY-DAY] HH:MM}**  
**no periodic {daily HH:MM to HH:MM | weekly WEEKLY-DAY HH:MM to [WEEKLY-DAY] HH:MM}**

#### Параметры

<b>daily HH:MM to HH:MM</b>	Укажите время в формате ЧЧ:ММ (например, 18:30).
<b>weekly WEEKLY-DAY HH:MM to [WEEKLY-DAY] HH:MM</b>	Укажите день недели (monday, tuesday, wednesday, thursday, friday, saturday, sunday) и время в формате ЧЧ:ММ. Конечный день недели, совпадающий с начальным, можно не указывать.

#### По умолчанию

Нет

#### Режим ввода команды

Time-range Configuration Mode

#### Использование команды

Новый период может частично совпадать с предыдущим. Если начало и завершение нового периода соответствуют началу и завершению предыдущего периода, будет отображено сообщение об ошибке и новый период не будет задан. При удалении необходимо полностью указать заданный ранее период. Если период указан не полностью или указано сразу несколько периодов, будет отображено сообщение об ошибке.

#### Пример

В данном примере показано, как создать временной интервал, включающий промежутки с 09:00 до 12:00 ежедневно и с 00:00 субботы до 00:00 понедельника, а также как удалить период с 09:00 до 12:00 ежедневно.

```
Switch# configure terminal
Switch(config)# time-range rdttime
Switch(config-time-range)# periodic daily 9:00 to 12:00
Switch(config-time-range)# periodic weekly saturday 00:00 to monday 00:00
Switch(config-time-range)# no periodic daily 9:00 to 12:00
Switch(config-time-range)#
```

### 65-2 show time-range

Данная команда используется для отображения конфигурации профиля диапазона времени.



**show time-range [NAME]****Параметры**

<i>NAME</i>	(Опционально) Укажите имя профиля диапазона времени, который необходимо отобразить.
-------------	---

**По умолчанию**

Нет

**Режим ввода команды**

EXEC Mode

**Использование команды**

Если параметр не указан, будут отображены все настроенные профили диапазона времени.

**Пример**

В данном примере показано, как отобразить все настроенные профили.

```
Switch#show time-range

Time Range Profile: rdtime
Daily 09:00 to 12:00
Weekly Saturday 00:00 to Monday 00:00

Time Range Profile: lunchtime
Daily 12:00 to 13:00

Total Entries: 2

Switch#
```

**65-3 time-range**

Данная команда используется для указания профиля диапазона времени и входа в режим Time-Range Configuration Mode. Используйте форму **no**, чтобы удалить временной диапазон.

**time-range NAME**  
**no time-range NAME**

**Параметры**

<i>NAME</i>	Укажите имя профиля диапазона времени, который необходимо настроить. Максимально допустимое количество символов – 32.
-------------	---

### По умолчанию

Нет

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте данную команду, чтобы войти в режим Time-Range Configuration Mode. Команду следует применять перед командой **periodic**, используемой для указания временного диапазона. Если временной диапазон создается без какой-либо настройки, это означает, что для данного временного диапазона нет активного периода, и отобразить его с помощью команды **show time-range** не получится.

### Пример

В данном примере показано, как войти в режим Time-Range Configuration Mode для профиля диапазона времени с именем «rdtime».

```
Switch# configure terminal
Switch(config)# time-range rdtime
Switch(config-time-range)#
```

## 66. Команды Traffic Segmentation

### 66-1 show traffic-segmentation forward

Данная команда используется для отображения конфигурации Traffic Segmentation на указанных или всех портах.

**show traffic-segmentation forward [interface *INTERFACE-ID* [, | -]]**

#### Параметры

<b>interface <i>INTERFACE-ID</i></b>	(Опционально) Укажите интерфейсы, которые будут отображаться.
<b>,</b>	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
<b>-</b>	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

#### По умолчанию

Нет

#### Режим ввода команды

EXEC Mode

#### Использование команды

Если параметр не указан, будет отображена конфигурация Traffic Segmentation для всех портов.

#### Пример

В данном примере показано, как отобразить конфигурацию Traffic Segmentation для интерфейса Ethernet 1/0/1.

```
Switch# show traffic-segmentation forward interface eth1/0/1

Interface          Forwarding Domain
-----
eth1/0/1           eth1/0/2,1/0/4-1/0/6

Total Entries: 1

Switch#
```

### 66-2 traffic-segmentation forward

Данная команда используется для ограничения продвижения пакетов в L2 домене, приходящих на настроенный порт. Используйте форму **no**, чтобы удалить ограничения продвижения пакетов в L2 домене.

**traffic-segmentation forward interface** *INTERFACE-ID* [, | -]  
**no traffic-segmentation forward interface** *INTERFACE-ID* [, | -]

### Параметры

<i>INTERFACE-ID</i>	Укажите разрешенные интерфейсы необходимых физических портов.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

### По умолчанию

Нет

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Если домен продвижения пакетов задан Traffic Segmentation, то пакеты, получаемые портом, будут ограничены пакетами, отправленными интерфейсами внутри заданного L2 домена. Если ограничение продвижения пакетов в домене L2 не указано, то получение портом пакетов не ограничено.

Команду **traffic-segmentation forward** можно использовать несколько раз. Все последующие интерфейсы будут добавлены в список участников домена. Используйте форму **no**, чтобы удалить указанный интерфейс из данного списка.

В список участников Traffic Segmentation могут входить различные типы интерфейсов, например, порт и port-channel в одном домене. Если интерфейсы, указанные командой, включают port-channel, все порты-участники данного port-channel будут добавлены в список участников домена.

Если домен продвижения пакетов для интерфейса не указан, то ограничений на продвижение пакетов на указанном порту нет.

### Пример

В данном примере показано, как настроить Traffic Segmentation и ограничить домен лавинной рассылки для Ethernet-порта 1/0/1. Установленное ограничение: от Ethernet-порта 1/0/3 до Ethernet- порта 1/0/6.

```
Switch# configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#traffic-segmentation forward interface ethernet 1/0/3-6
Switch(config-if)#
```

## 67. Команды Virtual LAN (VLAN)

### 67-1 acceptable-frame

Данная команда используется для настройки допустимых типов кадров на порту. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
acceptable-frame {tagged-only | untagged-only | admit-all}
no acceptable-frame
```

#### Параметры

<b>tagged-only</b>	Допускаются только тегированные кадры.
<b>untagged-only</b>	Допускаются только нетегированные кадры.
<b>admit-all</b>	Допускаются все кадры.

#### По умолчанию

Для режима access VLAN mode опцией по умолчанию является **untagged-only**.  
Для режима other VLAN mode опцией по умолчанию является **admit-all**.

#### Режим ввода команды

Interface Configuration Mode

#### Использование команды

Данная команда используется для настройки допустимых типов кадров на порту.

#### Пример

В данном примере показано, как настроить допустимый тип кадров tagged-only для порта Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# acceptable-frame tagged-only
Switch(config-if)#
```

### 67-2 ingress-checking

Данная команда используется для включения проверки входящих кадров, получаемых портом. Используйте форму **no** для отключения проверки.

```
ingress-checking
no ingress-checking
```

#### Параметры

Нет

#### По умолчанию

По умолчанию данная опция включена.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Используйте данную команду для включения проверки входящих кадров, получаемых интерфейсом. При включенной проверке пакет будет отброшен в том случае, если принимающий порт не является членом VLAN, классифицированной для получаемого пакета.

### Пример

В данном примере показано, как настроить проверку входящего трафика для включенного порта Ethernet 1/0/1.

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

## 67-3 show-vlan

Данная команда используется для отображения параметров для всех настроенных VLAN или одной VLAN на коммутаторе.

**show vlan [VLAN-ID [, | -] | interface [INTERFACE-ID [, | -]] | mac-vlan]**

### Параметры

<b>VLAN-ID</b>	(Опционально) Список VLAN для отображения информации о портах- участниках. Если VLAN не указана, то отображаются все VLAN. Корректный диапазон: от 1 до 4094.
,	(Опционально) Диапазон VLAN или разделение VLAN от предыдущего диапазона. Перед и после запятой использование пробела недопустимо.
-	(Опционально) Диапазон VLAN. Перед дефисом и после дефиса использование пробела недопустимо.
<b>interface INTERFACE-ID</b>	(Опционально) Порт для отображения настроек, касающихся VLAN.
,	(Опционально) Диапазон интерфейсов или разделение интерфейсов от предыдущего диапазона. Перед и после запятой использование пробела недопустимо.
-	(Опционально) Диапазон интерфейсов. Перед дефисом и после дефиса использование пробела недопустимо.
<b>mac-vlan</b>	(Опционально) Указывается для отображения информации о VLAN на основе MAC-адресов.

По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Данная команда используется для отображения параметров для всех настроенных VLAN или одной VLAN на коммутаторе.

### Пример

В данном примере показано, как отобразить все текущие записи VLAN.

```
Switch#show vlan

VLAN 1
  Name : default
  Description :
  Tagged Member Ports   :
  Untagged Member Ports : eth1/0/1-1/0/28

Total Entries : 1

Switch#
```

В данном примере показано, как отобразить информацию о PVID, проверке входящих пакетов и допустимых типах кадров для ethernet 1/0/1-1/0/4.

```
Switch#show vlan interface eth1/0/1-1/0/4
```

```
eth1/0/1
```

```
VLAN mode           : Hybrid
Native VLAN         : 1
Hybrid untagged VLAN : 1
Hybrid tagged VLAN  :
Ingress checking    : Enabled
Acceptable frame type : Admit-All
Dynamic tagged VLAN  :
```

```
eth1/0/2
```

```
VLAN mode           : Hybrid
Native VLAN         : 1
Hybrid untagged VLAN : 1
Hybrid tagged VLAN  :
Ingress checking    : Enabled
Acceptable frame type : Admit-All
Dynamic tagged VLAN  :
```

```
eth1/0/3
```

```
VLAN mode           : Hybrid
Native VLAN         : 1
Hybrid untagged VLAN : 1
Hybrid tagged VLAN  :
Ingress checking    : Enabled
Acceptable frame type : Admit-All
Dynamic tagged VLAN  :
```

```
eth1/0/4
```

```
VLAN mode           : Hybrid
Native VLAN         : 1
Hybrid untagged VLAN : 1
Hybrid tagged VLAN  :
Ingress checking    : Enabled
Acceptable frame type : Admit-All
Dynamic tagged VLAN  :
```

```
Switch#
```



## 67-4 switchport access vlan

Данная команда используется для указания access VLAN для интерфейса. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
switchport access vlan VLAN-ID
no switchport access vlan
```

### Параметры

VLAN-ID	Access VLAN интерфейса.
---------	-------------------------

### По умолчанию

По умолчанию access VLAN является VLAN 1.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Данная команда вступает в силу, когда интерфейс настроен в режиме доступа (access mode) или режиме dot1q-tunnel mode. VLAN, указанная в качестве access VLAN, не должна обязательно существовать для настройки команды. Может быть указана только одна access VLAN. Следующая команда перезаписывает предыдущую команду.

### Пример

В данном примере показано, как настроить ethernet 1/0/1 в режиме доступа (access mode) с access VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1000
Switch(config-if)#
```

## 67-5 switchport hybrid allowed vlan

Данная команда используется для указания тегированных или нетегированных VLAN для гибридного порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
switchport hybrid allowed vlan {[add] {tagged | untagged} | remove} VLAN-ID [, | -]
no switchport hybrid allowed vlan
```

### Параметры

<b>add</b>	(Опционально) Порт, который будет добавлен в указанную(-ые) VLAN.
<b>tagged</b>	Указывает порт в качестве тегированного для указанной(-ых) VLAN.
<b>untagged</b>	Указывает порт в качестве нетегированного для указанной(-ых) VLAN.

<b>remove</b>	Порт, который будет удален из указанной(-ых) VLAN.
<b>VLAN-ID</b>	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.
<b>,</b>	(Опционально) Диапазон VLAN или разделение VLAN от предыдущего диапазона. Перед и после запятой использование пробела недопустимо.
<b>-</b>	(Опционально) Диапазон VLAN. Перед дефисом и после дефиса использование пробела недопустимо.

### По умолчанию

По умолчанию гибридный порт является нетегированным членом VLAN 1.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Настраивая команду hybrid VLAN несколько раз с разными VLAN ID порт может стать тегированным или нетегированным членом нескольких VLAN.

Когда разрешенная VLAN указана только как VLAN ID, следующая команда перезапишет предыдущую команду. Если новый нетегированный разрешенный список VLAN перекрывается с текущим списком тегированных разрешенных VLAN, то перекрывающаяся часть будет изменена на нетегированную разрешенную VLAN. С другой стороны, если новый список тегированных разрешенных VLAN перекрывается с текущим списком нетегированных разрешенных VLAN, то перекрывающаяся часть будет изменена на тегированную разрешенную VLAN. Последняя команда вступит в силу. VLAN не должна обязательно существовать для настройки команды.

### Пример

В данном примере показано, как настроить ethernet 1/0/1 в качестве тегированного порта VLAN 1000 и нетегированного порта VLAN 2000 и 3000.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode hybrid
Switch(config-if)# switchport hybrid allowed vlan add tagged 1000
Switch(config-if)# switchport hybrid allowed vlan add untagged 2000,3000
Switch(config-if)#
```

## 67-6 switchport hybrid native vlan

Данная команда используется для указания native VLAN ID гибридного порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
switchport hybrid native vlan VLAN-ID
no switchport hybrid native vlan
```

### Параметры

---

VLAN-ID Native VLAN гибридного порта.

---

**По умолчанию**

По умолчанию native VLAN гибридного порта является VLAN 1.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

При настройке привязки гибридного порта к его native VLAN используйте команду **switchport hybrid allowed vlan**, чтобы добавить native VLAN в ее разрешенную VLAN. Указанная VLAN не должна обязательно существовать для применения этой команды. Команда вступает в силу, когда интерфейс настроен в гибридном режиме.

**Пример**

В данном примере показано, как настроить ethernet 1/0/1, чтобы он стал гибридным интерфейсом, и настроить PVID 20.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode hybrid
Switch(config-if)# switchport hybrid allowed vlan add untagged 1000,20
Switch(config-if)# switchport hybrid native vian 20
Switch(config-if)#
```

**67-7 switchport mode**

Данная команда используется для указания режима VLAN (VLAN mode) для порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
switchport mode {access | hybrid | trunk}
no switchport mode
```

**Параметры**

<b>access</b>	Указывает порт в качестве порта доступа.
<b>hybrid</b>	Указывает порт в качестве гибридного порта.
<b>trunk</b>	Указывает порт в качестве trunk-порта.

**По умолчанию**

По умолчанию установлена опция **hybrid**.

**Режим ввода команды**

Interface Configuration Mode

**Использование команды**

Когда порт установлен в режим доступа (access mode), этот порт будет нетегированным членом access VLAN, настроенной для порта. Когда порт установлен в гибридный режим (hybrid mode), порт может быть нетегированным или тегированным членом всех настроенных VLAN. Цель этого режима VLAN - поддержка protocol VLAN, VLAN на основе подсетей (subnet-based VLAN) и VLAN на основе MAC-адресов (MAC-based VLAN).

Когда порт настроен в режим trunk, этот порт является либо тегированным, либо нетегированным членом его native VLAN и может быть тегированным членом других настроенных VLAN. Цель trunk- порта - поддержка соединения switch-to-switch. Когда порт установлен в режим dot1q-tunnel mode, порт действует как порт UNI в service VLAN.

При изменении режима switch-port mode настройки, связанные с VLAN и ассоциированные с предыдущим режимом, будут утеряны.

### Пример

В данном примере показано, как настроить ethernet 1/0/1 в качестве trunk-порта.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)#
```

## 67-8 switchport trunk allowed vlan

Данная команда используется для настройки VLAN, которым разрешено получать и отправлять трафик на указанный интерфейс в тегированном формате. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**switchport trunk allowed vlan {all | [add | remove | except] VLAN-ID [, | -]}**  
**no switchport trunk allowed vlan**

### Параметры

<b>all</b>	VLAN, которые разрешены на интерфейсе.
<b>add</b>	Добавление списка указанных VLAN в список разрешенных VLAN.
<b>remove</b>	Удаление списка указанных VLAN из списка разрешенных VLAN.
<b>except</b>	Указывает, что разрешены все VLAN, за исключением VLAN, находящихся в списке исключений.
<b>VLAN-ID</b>	Список разрешенных VLAN или список VLAN, которые должны быть добавлены в список разрешенных VLAN или удалены из него.
<b>,</b>	(Опционально) Диапазон VLAN или разделение VLAN от предыдущего диапазона. Перед и после запятой использование пробела недопустимо.
<b>-</b>	(Опционально) Диапазон VLAN. Перед дефисом и после дефиса использование пробела недопустимо.

### По умолчанию

По умолчанию все VLAN разрешены.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Данная команда вступает в силу, только когда интерфейс настроен в режиме trunk mode. Если VLAN разрешена на trunk-порту, то порт станет тегированным членом VLAN. Когда для разрешенной VLAN установлена опция all, то порт будет автоматически добавлен во все VLAN, созданные системой.

### Пример

В данном примере показано, как настроить ethernet 1/0/1 в качестве тегированного члена VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 1000
Switch(config-if)#
```

## 67-9 switchport trunk native vlan

Данная команда используется для указания native VLAN ID интерфейса в режиме trunk mode. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
switchport trunk native vlan {VLAN-ID | tag}
no switchport trunk native vlan [tag]
```

### Параметры

<b>VLAN-ID</b>	Native VLAN для trunk-порта.
<b>tag</b>	Включение режима тегирования (tagging mode) native VLAN.

### По умолчанию

По умолчанию задана native VLAN 1, режим нетегированный.

### Режим ввода команды

Interface Configuration Mode

### Использование команды

Команда вступает в силу, только когда интерфейс настроен в режиме trunk 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)#
```

## 67-10 vlan

Данная команда используется для добавления VLAN и входа в режим VLAN Configuration Mode. Используйте форму **no** для удаления VLAN.

```
vlan VLAN-ID [, | -]
no vlan VLAN-ID [, | -]
```

### Параметры

VLAN-ID	Идентификатор VLAN, которая должны быть добавлена, удалена или настроена. Корректный диапазон VLAN ID: от 1 до 4094. VLAN ID 1 не может быть удален.
,	(Опционально) Диапазон VLAN или разделение VLAN от предыдущего диапазона. Перед и после запятой использование пробела недопустимо.
-	(Опционально) Диапазон VLAN. Перед дефисом и после дефиса использование пробела недопустимо.

### По умолчанию

VLAN ID 1 существует в системе в качестве VLAN по умолчанию.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Используйте команду глобальной настройки **vlan** для создания VLAN. Ввод команды **vlan** с VLAN ID влечет вход в режим настройки VLAN (VLAN configuration mode). Ввод VLAN ID существующей VLAN не создает новую VLAN, но разрешает пользователю изменить параметры VLAN для указанной VLAN. Когда пользователь вводит VLAN ID новой VLAN, VLAN будет создана автоматически.

Используйте команду **no vlan** для удаления VLAN. VLAN по умолчанию не может быть удалена. Если удаленная VLAN является access VLAN порта, то access VLAN порта будет сброшена в VLAN 1.

### Пример

В данном примере показано, как добавить новые VLAN, назначив новые VLAN с VLAN ID от 1000 до 1005.

```
Switch# configure terminal
Switch(config)# vlan 1000-1005
Switch(config-vlan)#
```

## 67-11 name

Данная команда используется для указания имени VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
name VLAN-NAME
no name
```

### Параметры

<i>VLAN-NAME</i>	Имя VLAN (макс. 32 символа). Имя VLAN должно быть уникальным в административном домене.
------------------	---

### По умолчанию

По умолчанию именем VLAN является VLANx, где x - четыре цифры (включая начальные нули), которые равны VLAN ID.

### Режим ввода команды

VLAN Configuration Mode

### Использование команды

Используйте данную команду для указания имени VLAN. Имя VLAN должно быть уникальным в административном домене.

### Пример

В данном примере показано, как настроить имя VLAN «admin-vlan» для VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# name admin-vlan
Switch(config-vlan)#
```

## 68. Команды Voice VLAN

### 68-1 voice vlan

Данная команда используется для глобального включения функции Voice VLAN и её настройки. Используйте форму **no**, чтобы отключить функцию Voice VLAN.

```
voice vlan VLAN-ID
no voice vlan
```

#### Параметры

VLAN-ID	Укажите VLAN ID голосовой VLAN в диапазоне от 2 до 4094.
---------	--

#### По умолчанию

По умолчанию данная функция отключена.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте данную команду для глобального включения функции Voice VLAN и её настройки. На коммутаторе может быть настроена только одна Voice VLAN.

Для включения функции Voice VLAN необходимо применить команду **voice vlan** в режиме Global Configuration Mode и команду **voice vlan enable** в режиме Interface Configuration Mode.

При включении на порту функции Voice VLAN полученные голосовые пакеты будут перенаправлены в данную Voice VLAN. При соответствии MAC-адресов источника пакетов адресам уникального идентификатора организации (OUI), настроенным при помощи команды **voice vlan mac-address**, полученные пакеты распознаются как голосовые пакеты.

Настройки Voice VLAN можно применить только к уже существующей VLAN. Настроенную Voice VLAN нельзя удалить с помощью команды **no vlan**.

#### Пример

В данном примере показано, как включить функцию Voice VLAN и настроить VLAN 1000 в качестве Voice VLAN.

```
Switch# configure terminal
Switch(config)# voice vlan 1000
Switch(config)#
```

### 68-2 voice vlan aging



Данная команда используется для настройки времени устаревания (Aging Time) для устаревших динамических Member-портов Voice VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**voice vlan aging MINUTES**  
**no voice vlan aging**

#### Параметры

<i>MINUTES</i>	Укажите время устаревания Voice VLAN в диапазоне от 1 до 65535 минут.
----------------	---

#### По умолчанию

Значение по умолчанию – 720 минут.

#### Режим ввода команды

Global Configuration Mode

#### Использование команды

Используйте данную команду для настройки времени устаревания для VoIP-устройства и автоматически изученных Member-портов Voice VLAN. Когда последнее VoIP-устройство, подключенное к порту, перестает отправлять трафик и MAC-адрес данного устройства устаревает в FDB, запускается таймер времени устаревания Voice VLAN. По истечении данного времени порт будет удален из Voice VLAN. Если голосовой трафик возобновляется в течение времени устаревания, таймер будет отменен.

#### Пример

В данном примере показано, как настроить время устаревания Voice VLAN на 30 минут.

```
Switch# configure terminal
Switch(config)# voice vlan aging 30
Switch(config)#
```

### 68-3 voice vlan enable

Данная команда используется для включения функции Voice VLAN на портах. Используйте форму **no**, чтобы отключить функцию Voice VLAN на портах.

**voice vlan enable**  
**no voice vlan enable**

#### Параметры

Нет

#### По умолчанию

По умолчанию данная функция отключена.

#### Режим ввода команды

## Interface Configuration Mode

**Использование команды**

Команда действует для портов доступа или гибридных портов. Используйте команду **voice vlan enable**, чтобы включить функцию голосовой VLAN для портов. Как команда **voice vlan** в глобальной конфигурации, так и команда **voice vlan enable** в режиме конфигурации интерфейса должны быть включены для порта, чтобы запустить функцию голосовой VLAN.

**Пример**

В данном примере показано, как включить функцию Voice VLAN на физическом порту Ethernet 1/0/1.

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

**68-4 voice vlan mac-address**

Данная команда используется для добавления уникального идентификатора организации (OUI), определяемого с устройства системы IP-телефонии. Используйте форму **no**, чтобы удалить OUI устройства системы IP-телефонии.

**voice vlan mac-address** *MAC-ADDRESS MASK* [**description** *TEXT*]  
**no voice vlan mac-address** *MAC-ADDRESS MASK*

**Параметры**

<i>MAC-ADDRESS</i>	Укажите MAC-адрес OUI.
<i>MASK</i>	Укажите соответствующую битовую маску MAC-адреса OUI.
<b>description</b> <i>TEXT</i>	(Опционально) Укажите описание OUI. Максимально допустимое количество символов – 32.

**По умолчанию**

OUI по умолчанию указаны в следующей таблице:

<b>OUI</b>	<b>Vendor</b>
00:E0:BB	ЗCOM
00:03:6B	Cisco
00:E0:75	Veritel
00:D0:1E	Pingtel
00:01:E3	Siemens
00:60:B9	NEC/Philips
00:0F:E2	Huawei-ЗCOM
00:09:6E	Avaya

**Режим ввода команды**

Global Configuration Mode

## Использование команды

Используйте данную команду для добавления уникального идентификатора организации (OUI), определяемого с устройства системы IP-телефонии. OUI используется для идентификации VoIP- трафика с помощью функции Voice VLAN. Если MAC-адреса источника полученных пакетов соответствуют любому из шаблонов OUI, полученные пакеты распознаются как VoIP-пакеты.

OUI, определяемый с устройства системы IP-телефонии, не может совпадать с OUI по умолчанию. OUI по умолчанию не может быть удален.

## Пример

В данном примере показано, как добавить OUI для устройства системы IP-телефонии.

```
Switch# configure terminal
Switch(config)# voice vlan mac-address 00-02-03-00-00-00 FF-FF-FF-00-00-00 description User1
Switch(config)#
```

## 68-5 voice vlan mode

Данная команда используется для включения автоматического изучения порта в качестве Member- порта Voice VLAN. Используйте форму **no**, чтобы отключить автоматическое изучение.

```
voice vlan mode {manual | auto {tag | untag}}
no voice vlan mode
```

## Параметры

<b>manual</b>	Укажите, чтобы настроить членство Voice VLAN вручную.
<b>auto</b>	Укажите, чтобы изучить участников Voice VLAN автоматически.
<b>tag</b>	Укажите, чтобы изучить тегированных участников Voice VLAN.
<b>untag</b>	Укажите, чтобы изучить нетегированных участников Voice VLAN.

## По умолчанию

Параметры по умолчанию – **untag** или **auto**.

## Режим ввода команды

Interface Configuration Mode

## Использование команды

Используйте данную команду, чтобы настроить автоматическое изучение Member-портов Voice VLAN или назначить их вручную.

Если автоматическое изучение включено, порт будет автоматически распознан в качестве участника Voice VLAN. В дальнейшем участники будут автоматически удалены согласно времени устаревания. Когда порт работает в автотегированном режиме (**Auto Tagged Mode**) и фиксирует VoIP-устройство через OUI, он автоматически присоединится к Voice VLAN как тегированный порт. Если VoIP- устройство отправляет

тегированные пакеты, коммутатор изменит их приоритет. Нетегированные пакеты отправляются в PVID VLAN порта.

Когда порт работает в автонетегированном режиме (**Auto Untagged Mode**) и получает информацию о VoIP-устройстве через OUI, он автоматически присоединится к Voice VLAN как нетегированный порт. Если VoIP-устройство отправляет тегированные пакеты, коммутатор изменит их приоритет. Нетегированные пакеты отправляются в Voice VLAN.

Когда коммутатор принимает пакеты LLDP-MED, он проверяет VLAN ID, флаги тега и приоритета, настройкам которых он должен следовать.

Если автоматическое изучение отключено, используйте команду **switchport hybrid vlan** для настройки порта в качестве тегированного или нетегированного Member-порта Voice VLAN.

### Пример

В данном примере показано, как настроить автотегированный режим (**Auto Tagged Mode**) на физическом порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# voice vlan mode auto tag
Switch(config-if)#
```

## 68-6 voice vlan qos

Данная команда используется для настройки приоритета CoS для входящего трафика Voice VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
voice vlan qos COS-VALUE
no voice vlan qos
```

### Параметры

<i>COS-VALUE</i>	Укажите приоритет Voice VLAN в диапазоне от 0 до 7.
------------------	---

### По умолчанию

Значение по умолчанию – 5.

### Режим ввода команды

Global Configuration Mode

### Использование команды

Данная команда используется для маркировки CoS голосовых пакетов, поступающих на порт, на котором включена Voice VLAN. Маркировка CoS позволяет отделить голосовой трафик от трафика данных по качеству обслуживания.

### Пример

В данном примере показано, как настроить приоритет Voice VLAN со значением 7.

```
Switch# configure terminal
Switch(config)# voice vlan qos 7
Switch(config)#
```

## 68-7 show voice vlan

Данная команда используется для отображения настроек Voice VLAN.

```
show voice vlan [interface [INTERFACE-ID [, | -]]]
show voice vlan {device | lldp-med device} [interface INTERFACE-ID [, | -]]
```

### Параметры

<b>interface</b>	(Опционально) Указывает на отображение информации о голосовой VLAN для портов.
<b>interface</b> <i>INTERFACE-ID</i>	(Опционально) Указывает интерфейс для отображения.
<b>,</b>	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
<b>-</b>	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
<b>device</b>	Укажите, чтобы отобразить VoIP-устройства, информация о которых была получена через OUI.
<b>lldp-med device</b>	Укажите, чтобы отобразить VoIP-устройства, обнаруженные через LLDP-MED.

### По умолчанию

Нет

### Режим ввода команды

EXEC Mode

### Использование команды

Данная команда используется для отображения настроек Voice VLAN.

### Пример

В данном примере показано, как отобразить глобальные настройки Voice VLAN.

```
Switch# show voice vlan

Voice VLAN ID      : 1000
Voice VLAN CoS     : 7
Aging Time         : 30 minutes
Member Ports       : eth1/0/1-1/0/5
Dynamic Member Ports : eth1/0/1-1/0/3
Voice VLAN OUI:

OUI Address      Mask      Description
-----
00-01-E3-00-00-00 FF-FF-FF-00-00-00 Siemens
00-03-6B-00-00-00 FF-FF-FF-00-00-00 Cisco
00-09-6E-00-00-00 FF-FF-FF-00-00-00 Avaya
00-0F-E2-00-00-00 FF-FF-FF-00-00-00 Huawei&3COM
00-60-B9-00-00-00 FF-FF-FF-00-00-00 NEC&Philips
00-D0-1E-00-00-00 FF-FF-FF-00-00-00 Pingtel
00-E0-75-00-00-00 FF-FF-FF-00-00-00 Veritel
00-E0-BB-00-00-00 FF-FF-FF-00-00-00 3COM
00-02-03-00-00-00 FF-FF-FF-00-00-00 User1

Total OUI: 9

Switch#
```

В данном примере показано, как отобразить информацию о портах Voice VLAN.

```
Switch# show voice vlan interface eth1/0/1-5

Interface      State      Mode
-----
eth1/0/1       Enabled    Auto/Tag
eth1/0/2       Enabled    Manual
eth1/0/3       Enabled    Manual
eth1/0/4       Enabled    Auto/Untag
eth1/0/5       Disabled   Manual

Switch#
```

В этом примере показано, как отобразить изученные голосовые устройства на портах 1 - 2.

```
Switch# show voice vlan device interface eth1/0/1-2
```

Interface	Device Address	Start Time	Status
eth1/0/1	00-03-6B-00-00-01	2012-03-19 09:00	Active
eth1/0/1	00-03-6B-00-00-02	2012-03-20 10:09	Aging
eth1/0/1	00-03-6B-00-00-05	2012-03-20 12:04	Active
eth1/0/2	00-03-6B-00-00-0a	2012-03-19 08:11	Aging
eth1/0/2	33-00-61-10-00-11	2012-03-20 06:45	Aging

```
Total Entries: 5
```

```
Switch#
```

В данном примере показано, как отобразить VoIP-устройства, обнаруженные через LLDP-MED, на Eth-портах 1/0/1-1/0/2.

```
Switch# show voice vlan lldp-med device interface eth1/0/1-2
```

```
Index          : 1
Interface      : eth1/0/1
Chassis ID Subtype : MAC Address
Chassis ID     : 00-E0-BB-00-00-11
Port ID Subtype : Network Address
Port ID        : 172.18.1.1
Create Time    : 2012-03-19 10:00
Remain Time    : 108 Seconds
```

```
Index          : 2
Interface      : eth1/0/2
Chassis ID Subtype : MAC Address
Chassis ID     : 00-E0-BB-00-00-12
Port ID Subtype : Network Address
Port ID        : 172.18.1.2
Create Time    : 2012-03-20 11:00
Remain Time    : 105 Seconds
```

```
Total Entries: 2
```

```
Switch#
```

## Приложение А - Записи системного журнала

В следующей таблице перечислены все возможные записи и их соответствующие значения, которые будут отображаться в системном журнале данного коммутатора.

### 802.1X

Описание записей журнала	Уровень
<p>Описание события: Сбой аутентификации 802.1X.</p> <p>Сообщение журнала: Сбой проверки подлинности 802.1X [из-за &lt;причины&gt;] с (Имя пользователя: &lt;username&gt;, &lt;interface-id&gt;, MAC: &lt;mac-address&gt;)</p> <p>Параметры Описание:</p> <p>reason: Причина неудачной аутентификации. Возможными причинами могут быть:</p> <p>(1) user authentication failure.</p> <p>(2) no server(s) responding.</p> <p>(3) no servers configured.</p> <p>(4) no resources.</p> <p>(5) user timeout expired.</p> <p>имя пользователя: пользователь, проходящий аутентификацию.</p> <p>interface-id: Номер интерфейса коммутатора.</p> <p>mac-адрес: MAC-адрес аутентифицируемого устройства.</p>	Критический
<p>Описание события: Аутентификация 802.1X успешна.</p> <p>Сообщение журнала: 802.1X authentication success (Username: &lt;username&gt;, &lt;interface-id&gt;, MAC: &lt;mac-address&gt;)</p> <p>Параметры Описание:</p> <p>имя пользователя: пользователь, который проходит проверку подлинности.</p> <p>interface-id: Имя интерфейса.</p> <p>mac-адрес: MAC-адрес аутентифицируемого устройства.</p>	Информационный

### AAA

Описание записей журнала	Уровень
<p>Описание события: Этот журнал будет создан, когда глобальное состояние AAA включено или отключено.</p> <p>Сообщение журнала: AAA - &lt;статус&gt;</p> <p>Параметры Описание:</p> <p>status: Статус указывает на то, что AAA включен или отключен.</p>	Информационный
<p>Описание события: Этот журнал будет создан при успешном входе в систему.</p> <p>Сообщение журнала: Успешный вход через &lt;exec-type&gt; [from &lt;client-ip&gt;]authenticated by AAA &lt;aaa-method&gt; (Username:</p>	Предупреждение



---

<username>)

Параметры Описание:

exec-type: Указывает типы EXEC. Например, Console, Telnet, SSH, Web и Web (SSL).

client-ip: Указывает IP-адрес клиента, если он действителен по протоколу IP. aaa-method: Указывает метод аутентификации. Например, none и local.

Username: Указывает имя пользователя для аутентификации.

Note: Для консоли не будет информации об IP-адресе клиента для регистрации.

---

Описание события: Этот журнал будет создан при сбое входа в систему. Предупреждение

Сообщение журнала: Не удалось войти в систему через <exec-type> [from <client-ip>]authenticated by AAA <aaa-method> (Username: <username>)

Параметры Описание:

exec-type: Указывает типы EXEC. Например, Console, Telnet, SSH, Web и Web (SSL).

client-ip: Указывает IP-адрес клиента, если он действителен по протоколу IP. aaa-method: Указывает метод аутентификации. Например, локальный.

username: Указывает имя пользователя для аутентификации.

Note: Для консоли не будет информации об IP-адресе клиента для регистрации.

---

## Auto Surveillance VLAN

Описание записей журнала	Уровень
<p>Описание события: При обнаружении нового устройства наблюдения на интерфейсе.</p> <p>Сообщение журнала: Обнаружено новое устройство наблюдения (&lt;interface-id&gt;, MAC: &lt;mac-address&gt;) Параметры Описание:</p> <p>interface-id: Имя интерфейса.</p> <p>mac-адрес: MAC-адрес устройства наблюдения.</p>	Информационный
<p>Описание события: Когда интерфейс, на котором включено наблюдение, VLAN автоматически присоединяется к VLAN наблюдения.</p> <p>Log Message: &lt;interface-id&gt; add into surveillance VLAN &lt;vid&gt;</p> <p>Parameters Description:</p> <p>interface-id: Имя интерфейса.</p> <p>vid: идентификатор виртуальной локальной сети.</p>	Информационный
<p>Описание события: Когда интерфейс покидает сеть VLAN наблюдения и в то же время в интервале старения для этого интерфейса не обнаружено ни одного устройства наблюдения, будет отправлено сообщение журнала.</p> <p>Сообщение журнала: &lt;interface-id&gt; remove from surveillance VLAN &lt;vid&gt; Описание параметров:</p> <p>interface-id: Имя интерфейса.</p>	Информационный

vid: идентификатор виртуальной локальной сети.	
<p>Описание события: Когда IPC добавляется в VLAN наблюдения, отправляется сообщение журнала.</p> <p>Сообщение журнала: ASV: Add IPC(&lt;ipaddr&gt;) Описание параметров:</p> <p>ipaddr: Представляет собой IP-адрес IPC.</p>	Информационный
<p>Описание события: Когда IPC удаляется из сети наблюдения VLAN, отправляется сообщение журнала.</p> <p>Сообщение журнала: ASV: Remove IPC(&lt;ipaddr&gt;) Параметры Описание:</p> <p>ipaddr: Представляет собой IP-адрес IPC.</p>	Информационный
<p>Описание события: Когда NVR добавляется в сеть VLAN наблюдения, отправляется сообщение журнала.</p> <p>Сообщение журнала: ASV: Add NVR(&lt;ipaddr&gt;) Описание параметров:</p> <p>ipaddr: Представляет собой IP-адрес сетевого видеорегистратора.</p>	Информационный
<p>Описание события: Когда сетевой видеорегистратор удаляется из сети наблюдения VLAN, отправляется сообщение журнала.</p> <p>Сообщение журнала: ASV: Remove NVR(&lt;ipaddr&gt;) Параметры Описание:</p> <p>ipaddr: Представляет собой IP-адрес сетевого видеорегистратора.</p>	Информационный
<p>Описание события: Когда режим ASV 2.0 изменяется с помощью Web GUI, отправляется сообщение журнала.</p> <p>Сообщение журнала: ASV: Изменение режима с &lt;мод&gt; на &lt;мод&gt;.</p> <p>Описание параметров:</p> <p>mode: Представляет собой режим ASV 2.0. Режим может быть стандартным или режимом наблюдения.</p>	Информационный

## Configuration/Firmware

Описание записей журнала	Уровень
<p>Описание события: Прошивка успешно обновлена.</p> <p>Сообщение журнала: Firmware upgraded by &lt;session&gt; successfully (Username: &lt;имя пользователя&gt;[, IP: &lt;ipaddr&gt;, MAC: &lt;macaddr&gt;], IP сервера: &lt;serverIP&gt;, Имя файла: &lt;pathFile&gt;)</p> <p>Параметры Описание:</p> <p>session: Сеанс пользователя.</p> <p>username (имя пользователя): Представляет текущего пользователя входа в систему.</p> <p>ipaddr: Представляет IP-адрес клиента.</p> <p>macaddr: Представляет MAC-адрес клиента.</p> <p>serverIP: IP-адрес сервера.</p> <p>pathFile: Путь и имя файла на сервере.</p>	Информационный

<p>Note: Для консоли информация об IP и MAC не будет использоваться для ведения журнала.</p>	
<p>Описание события: Неудачное обновление микропрограммы.  Сообщение журнала: Неудачное обновление микропрограммы &lt;сессией&gt; (Имя пользователя: &lt;имя пользователя&gt;[, IP: &lt;ipaddr&gt;, MAC: &lt;macaddr&gt;], IP сервера: &lt;serverIP&gt;, Имя файла: &lt;pathFile&gt;)  Параметры Описание:  session: Сеанс пользователя.  username (имя пользователя): Представляет текущего пользователя входа в систему.  ipaddr: Представляет IP-адрес клиента.  macaddr: Представляет MAC-адрес клиента.  serverIP: IP-адрес сервера.  pathFile: Путь и имя файла на сервере.  Note: Для консоли информация об IP и MAC не будет использоваться для ведения журнала.</p>	Предупреждение
<p>Описание события: Прошивка загружена успешно.  Сообщение журнала: Firmware uploaded by &lt;session&gt; successfully (Username: &lt;имя пользователя&gt;[, IP: &lt;ipaddr&gt;, MAC: &lt;macaddr&gt;], IP сервера: &lt;serverIP&gt;, Имя файла: &lt;pathFile&gt;)  Параметры Описание:  session: Сеанс пользователя.  username (имя пользователя): Представляет текущего пользователя входа в систему.  ipaddr: Представляет IP-адрес клиента.  macaddr: Представляет MAC-адрес клиента.  serverIP: IP-адрес сервера.  pathFile: Путь и имя файла на сервере.  Note: Для консоли информация об IP и MAC не будет использоваться для ведения журнала.</p>	Информационный
<p>Описание события: Неудачная загрузка микропрограммы.  Сообщение журнала: Прошивка загружена &lt;сессией&gt; неудачно (Имя пользователя: &lt;имя пользователя&gt;[, IP: &lt;ipaddr&gt;, MAC: &lt;macaddr&gt;], IP сервера: &lt;serverIP&gt;, Имя файла: &lt;pathFile&gt;)  Параметры Описание:  session: Сеанс пользователя.  username (имя пользователя): Представляет текущего пользователя. ipaddr: Представляет IP-адрес клиента.  macaddr: Представляет MAC-адрес клиента. serverIP: IP-адрес сервера.  pathFile: Путь и имя файла на сервере.  Note: Для консоли не будет информации об IP и MAC для регистрации.</p>	Предупреждение
<p>Описание события: Конфигурация загружена успешно.  Сообщение журнала: Конфигурация загружена &lt;сессией&gt;</p>	Информационный

успешно. (Имя пользователя: <имя пользователя>[, IP: <ipaddr>, MAC: <macaddr>], IP сервера: <serverIP>, Имя файла: <pathFile>)	
Параметры Описание: сессия: Сеанс пользователя. имя пользователя: Представляет текущего пользователя входа в систему. ipaddr: Представляет IP-адрес клиента. macaddr: Представляет MAC-адрес клиента. serverIP: IP-адрес сервера. pathFile: Путь и имя файла на сервере. Примечание: Для консоли информация об IP и MAC не будет использоваться для ведения журнала.	
Описание события: Конфигурация загружена неудачно. Сообщение журнала: Конфигурация загружена <сессией> неудачно. (Имя пользователя: <имя пользователя>[, IP: <ipaddr>, MAC: <macaddr>], IP сервера: <serverIP>, Имя файла: <pathFile>) Параметры Описание: сессия: Сеанс пользователя. имя пользователя: Представляет текущего пользователя входа в систему. ipaddr: Представляет IP-адрес клиента. macaddr: Представляет MAC-адрес клиента. serverIP: IP-адрес сервера. pathFile: Путь и имя файла на сервере. Примечание: Для консоли информация об IP и MAC не будет использоваться для ведения журнала.	Предупреждение
Описание события: Конфигурация загружена успешно. Сообщение журнала: Конфигурация загружена <сессией> успешно. (Имя пользователя: <имя пользователя>[, IP: <ipaddr>, MAC: <macaddr>], IP сервера: <serverIP>, Имя файла: <pathFile>) Параметры Описание: сессия: Сеанс пользователя. имя пользователя: Представляет текущего пользователя входа в систему. ipaddr: Представляет IP-адрес клиента. macaddr: Представляет MAC-адрес клиента. serverIP: IP-адрес сервера. pathFile: Путь и имя файла на сервере. Примечание: Для консоли информация об IP и MAC не будет использоваться для ведения журнала.	Информационный
Описание события: Конфигурация загружена неудачно. Сообщение журнала: Конфигурация загружена <сессией> неудачно. (Имя пользователя: <имя пользователя>[, IP: <ipaddr>, MAC: <macaddr>], IP сервера: <serverIP>, Имя файла: <pathFile>) Параметры Описание: сессия: Сеанс пользователя. имя пользователя: Представляет текущего пользователя входа в систему. ipaddr: Представляет IP-адрес клиента. macaddr: Представляет MAC-адрес клиента. serverIP: IP-адрес сервера. pathFile: Путь и имя файла на сервере. Примечание: Для консоли информация об IP и MAC не будет использоваться для ведения журнала.	Предупреждение

<p>Параметры Описание:</p> <p>сессия: Сеанс пользователя.</p> <p>имя пользователя: Представляет текущего пользователя.</p> <p>ipaddr: Представляет IP-адрес клиента. macaddr: Представляет MAC-адрес клиента.</p> <p>serverIP: IP-адрес сервера.</p> <p>pathFile: Путь и имя файла на сервере.</p> <p>Примечание: Для консоли не будет информации об IP и MAC для регистрации.</p>	
<p>Описание события: Конфигурация сохранена во флэш-память с помощью консоли.</p> <p>Сообщение в журнале: Configuration saved to flash by console (Username: &lt;username&gt;) Parameters Description:</p> <p>имя пользователя: Представляет текущего пользователя для входа в систему.</p>	Информационный
<p>Описание события: Конфигурация сохранена во флэш-память удаленным устройством.</p> <p>Сообщение журнала: Configuration saved to flash (Username: &lt;username&gt;, IP: &lt;ipaddr&gt;) Parameters Description:</p> <p>имя пользователя: Представляет текущего пользователя для входа в систему.</p> <p>ipaddr: Представляет IP-адрес клиента.</p>	Информационный
<p>Описание события: Сообщение журнала успешно загружено.</p> <p>Сообщение журнала: Сообщение журнала успешно загружено &lt;сессией&gt;. (Имя пользователя: &lt;username&gt;[, IP: &lt;ipaddr&gt;, MAC: &lt;macaddr&gt;])</p> <p>Параметры Описание:</p> <p>сессия: Сеанс пользователя.</p> <p>имя пользователя: Представление текущего пользователя при входе в систему.</p> <p>ipaddr: Представляет IP-адрес клиента.</p> <p>macaddr: Представляет MAC-адрес клиента.</p> <p>Примечание: Для консоли информация об IP и MAC не будет использоваться для регистрации.</p>	Информационный
<p>Описание события: Сообщение журнала загружено неудачно.</p> <p>Сообщение журнала: Сообщение журнала загружено &lt;сессией&gt; неудачно. (Имя пользователя: &lt;username&gt;[, IP: &lt;ipaddr&gt;, MAC: &lt;macaddr&gt;])</p> <p>Параметры Описание:</p> <p>сессия: Сеанс пользователя.</p> <p>имя пользователя: Представление текущего пользователя при входе в систему.</p> <p>ipaddr: Представляет IP-адрес клиента.</p> <p>macaddr: Представляет MAC-адрес клиента.</p> <p>Примечание: Для консоли информация об IP и MAC не будет использоваться для регистрации.</p>	Предупреждение
<p>Описание события: Неудачно загружены файлы неизвестного типа.</p>	Предупреждение

Сообщение журнала: Загружено <сессией> неудачно. (Имя пользователя: <имя пользователя>[, IP: <ipaddr>, MAC: <macaddr>], IP сервера: <serverIP>, Имя файла: <pathFile>)

Параметры Описание:

сессия: Сеанс пользователя.

имя пользователя: Представляет текущего пользователя входа в систему.

ipaddr: Представляет IP-адрес клиента.

macaddr: Представляет MAC-адрес клиента.

serverIP: IP-адрес сервера.

pathFile: Путь и имя файла на сервере.

Примечание: Для консоли информация об IP и MAC не будет использоваться для ведения журнала.



**Примечание:**

1. Сеанс пользователя указывает на Console, Web, SNMP, Telnet или SSH.
2. При обновлении конфигурации/прошивки через консоль информация об IP и MAC не будет заноситься в журнал.

## DAI

Описание записей журнала	Уровень
<p>Описание события: Этот журнал создается, когда DAI обнаруживает недействительный ARP-пакет.</p> <p>Сообщение журнала: Незаконные ARP &lt;тип&gt; пакеты (IP: &lt;ip-address&gt;, MAC: &lt;mac-address&gt;, VLAN &lt;vlan-id&gt;, on &lt;interface-id&gt;).</p> <p>Параметры Описание:</p> <p>type: Тип ARP-пакета, он указывает, является ли ARP-пакет запросом или ARP-ответом.</p>	Предупреждение
<p>Описание события: Этот журнал будет создан, когда DAI обнаружит действительный ARP-пакет.</p> <p>Сообщение журнала: Законные ARP &lt;тип&gt; пакеты (IP: &lt;ip-address&gt;, MAC: &lt;mac-address&gt;, VLAN &lt;vlan-id&gt;, on &lt;interface-id&gt;).</p> <p>Параметры Описание:</p> <p>type: Тип ARP-пакета, он указывает на то, что ARP-пакет является запросом или ARP-ответом.</p>	Информационный

## DHCPv6 Client

Описание записей журнала	Уровень
<p>Описание события: Изменено состояние администратора интерфейса клиента DHCPv6.</p> <p>Сообщение журнала: Клиент DHCPv6 на интерфейсе &lt;interface-name&gt; изменил состояние на [enabled   disabled].</p> <p>Параметры Описание:</p>	Информационный

ipif-name: имя интерфейса клиента DHCPv6.	
<p>Описание события: Клиент DHCPv6 получает IPv6-адрес от сервера DHCPv6.</p> <p>Сообщение журнала: Клиент DHCPv6 получает ipv6-адрес &lt;ipv6address&gt; на интерфейсе &lt;ipif-name&gt;.</p> <p>Параметры Описание:</p> <p>ipv6address: IPv6-адрес, полученный от сервера DHCPv6. ipif-name: Имя интерфейса клиента DHCPv6.</p>	Информационный
<p>Описание события: IPv6-адрес, полученный от сервера DHCPv6, начинает обновляться.</p> <p>Сообщение журнала: IPv6-адрес &lt;ipv6address&gt; на интерфейсе &lt;ipif-name&gt; начинает обновляться.</p> <p>Описание параметров:</p> <p>ipv6address: IPv6-адрес, полученный от сервера DHCPv6.</p> <p>ipif-name: Имя интерфейса клиента DHCPv6.</p>	Информационный
<p>Описание события: IPv6-адрес, полученный от сервера DHCPv6, успешно обновляется.</p> <p>Сообщение журнала: IPv6-адрес &lt;ipv6address&gt; на интерфейсе &lt;ipif-name&gt; обновлен успешно.</p> <p>Описание параметров:</p> <p>ipv6address: IPv6-адрес, полученный от сервера DHCPv6.</p> <p>ipif-name: Имя интерфейса клиента DHCPv6.</p>	Информационный
<p>Описание события: IPv6-адрес, полученный от сервера DHCPv6, начинает перепривязку.</p> <p>Сообщение журнала: IPv6-адрес &lt;ipv6address&gt; на интерфейсе &lt;ipif-name&gt; начинает перепривязку.</p> <p>Описание параметров:</p> <p>ipv6address: IPv6-адрес, полученный от сервера DHCPv6.</p> <p>ipif-name: Имя интерфейса клиента DHCPv6.</p>	Информационный
<p>Описание события: IPv6-адрес, полученный от сервера DHCPv6, успешно перепривязан.</p> <p>Сообщение журнала: IPv6-адрес &lt;ipv6address&gt; на интерфейсе &lt;ipif-name&gt; успешно перепривязан.</p> <p>Параметры Описание:</p> <p>ipv6address: IPv6-адрес, полученный от сервера DHCPv6.</p> <p>ipif-name: Имя интерфейса клиента DHCPv6.</p>	Информационный
<p>Описание события: IPv6-адрес с сервера DHCPv6 был удален.</p> <p>Сообщение журнала: IPv6-адрес &lt;ipv6address&gt; на интерфейсе &lt;ipif-name&gt; был удален</p> <p>Параметры Описание:</p> <p>ipv6address: IPv6-адрес, полученный от сервера DHCPv6.</p> <p>ipif-name: Имя интерфейса клиента DHCPv6.</p>	Информационный

## DHCPv6 Relay

Описание записей журнала	Уровень
Описание события: Изменено состояние администратора ретрансляции DHCPv6 на указанном интерфейсе.	Информационный

Сообщение журнала: DHCPv6 relay on interface <ipif-name> changed state to [enabled | disabled].

Параметры Описание:

ipif-name: имя интерфейса агента ретрансляции DHCPv6.

## DoS Prevention

Описание записей журнала	Уровень
<p>Описание события: Обнаружение DOS-атаки.</p> <p>Log Message: &lt;dos-type&gt; сброшен с (IP: &lt;ip-address&gt; Port &lt;interface-id&gt;)</p> <p>Параметры Описание:</p> <p>dos-type: Тип атаки DOS.</p> <p>ip-адрес: IP-адрес.</p> <p>interface-id: Имя интерфейса.</p>	Уведомление

## DNS Resolver

Описание записей журнала	Уровень
<p>Описание события: Добавлен дубликат кэша доменных имен, ведет к удалению динамического кэша доменных имен.</p> <p>Сообщение журнала: [DNS-RESOLVER(1):]Дубликат доменного имени имя случая: &lt;доменное имя&gt;, статический IP: &lt;ipaddr&gt;, динамический IP:&lt;ipaddr&gt;.</p> <p>Параметры Описание:</p> <p>domain-name: Строка доменного имени.</p> <p>ipaddr: IP-адрес.</p>	Информационный

## Interface

Описание записей журнала	Уровень
<p>Описание события: Когда порт не работает.</p> <p>Log Message: Порт &lt;port-type&gt;&lt;interface-id&gt; link down</p> <p>Параметры Описание:</p> <p>port-type: Тип порта.</p> <p>interface-id: Имя интерфейса.</p>	Информационный
<p>Описание события: Когда порт находится в рабочем состоянии.</p> <p>Log Message: Порт &lt;port-type&gt;&lt;interface-id&gt; link up, &lt;link-speed&gt;</p> <p>Параметры Описание:</p> <p>port-type: Тип порта.</p> <p>interface-id: Имя интерфейса.</p> <p>link-speed: Скорость соединения порта.</p>	Информационный
<p>Описание события: Порт связан в полудуплексном режиме.</p> <p>Log Message: ASV: Port &lt;interface-id&gt; Half duplex detected</p> <p>Параметры Описание:</p> <p>interface-id: Имя интерфейса.</p>	Предупреждение



## IPv6 Duplicate Address

Описание записей журнала	Уровень
<p>Описание события: Этот журнал будет создан, когда DUT получает сообщение Neighbor Solicitation (NS) с дублированным адресом в течение DAD.</p> <p>Сообщение журнала: Дублирование адреса &lt;ipv6address&gt; на &lt;interface-id&gt; через получение сообщений Neighbor Solicitation Messages.</p> <p>Параметры Описание:</p> <p>ipv6address: ipv6-адрес в сообщениях Neighbor Solicitation Messages</p> <p>interface-id: Имя интерфейса</p>	Предупреждение
<p>Описание события: Этот журнал будет создан, когда DUT получает сообщение Neighbor Advertisement (NA) с дублированным адресом в течение DAD.</p> <p>Сообщение журнала: Дублирование адреса &lt;ipv6address&gt; на &lt;interface-id&gt; через получение сообщений Neighbor Advertisement Messages.</p> <p>Параметры Описание:</p> <p>ipv6address: ipv6-адрес в сообщениях Neighbor Advertisement Messages</p> <p>interface-id: Имя интерфейса</p>	Предупреждение

## LACP

Описание записей журнала	Уровень
<p>Описание события: Link Aggregation Group link up.</p> <p>Сообщение журнала: Link Aggregation Group &lt;group_id&gt; link up</p> <p>Параметры Описание:</p> <p>group_id: Идентификатор группы агрегации каналов.</p>	Информационный
<p>Описание события: Неисправность соединения группы агрегации каналов.</p> <p>Сообщение журнала: Link Aggregation Group &lt;group_id&gt; link down</p> <p>Параметры Описание:</p> <p>group_id: Идентификатор группы агрегации каналов.</p>	Информационный
<p>Описание события: Порт-член присоединен к группе агрегации каналов. Log Message: &lt;ifname&gt; attach to Link Aggregation Group &lt;group_id&gt;</p> <p>Параметры Описание:</p> <p>ifname: имя интерфейса порта, который присоединяется к группе агрегации.</p> <p>group_id: Идентификатор группы агрегации, к которой присоединяется порт.</p>	Информационный
<p>Описание события: Порт-член отсоединяется от группы агрегации каналов. Log Message: &lt;ifname&gt; detach from Link Aggregation Group &lt;group_id&gt;</p> <p>Параметры Описание:</p> <p>ifname: имя интерфейса порта, который отсоединяется от группы агрегации.</p>	Информационный

---

group\_id: Идентификатор группы агрегации, от которой отсоединяется порт.

---

## LBD

Описание записей журнала	Уровень
<p>Описание события: Запись события, когда интерфейс обнаруживает петлю. Log Message: &lt;interface-id&gt; LBD loop occurred</p> <p>Описание параметров: interface-id: Интерфейс, на котором обнаружена петля.</p>	Критический
<p>Описание события: Запись события, когда интерфейс обнаруживает петлю. Log Message: &lt;interface-id&gt; VLAN &lt;vlan-id&gt; LBD loop occurred</p> <p>Описание параметров: interface-id: Интерфейс, на котором обнаружена петля. vlan-id: VLAN, в которой обнаружена петля.</p>	Критический
<p>Описание события: Запись события при восстановлении петли интерфейса. Log Message: &lt;interface-id&gt; LBD loop recovered</p> <p>Описание параметров: interface-id: Интерфейс, на котором обнаружена петля.</p>	Критический
<p>Описание события: Запись события при восстановлении петли интерфейса. Log Message: &lt;interface-id&gt; VLAN &lt;vlan-id&gt; LBD loop recovered</p> <p>Параметры Описание: interface-id: Интерфейс, на котором обнаружена петля. vlan-id: VLAN, в которой обнаружена петля.</p>	Критический
<p>Описание события: Запись события, когда количество VLAN, в которых произошла петля возврата, превышает зарезервированное число.</p> <p>Сообщение журнала: Переполнение номеров виртуальных локальных сетей</p>	Критический

## LLDP-MED

Описание записей журнала	Уровень
<p>Описание события: Обнаружено изменение топологии LLDP-MED.</p> <p>Сообщение журнала: Обнаружено изменение топологии LLDP-MED (на порту &lt;portNum&gt;. идентификатор шасси: &lt;chassisType&gt;, &lt;chassisID&gt;, идентификатор порта: &lt;portType&gt;, &lt;portID&gt;, класс устройства: &lt;deviceClass&gt;)</p> <p>Параметры Описание: portNum: Номер порта. chassisType: chassis ID subtype.</p> <p>Список значений: 1. chassisComponent(1)</p>	Уведомление

---

- 
- 2. interfaceAlias(2)
  - 3. portComponent(3)
  - 4. macAddress(4)
  - 5. networkAddress(5)
  - 6. interfaceName(6)
  - 7. local(7)

chassisID: chassis ID. portType: port ID subtype.

Список значений:

- 1. interfaceAlias(1)
- 2. portComponent(2)
- 3. macAddress(3)
- 4. networkAddress(4)
- 5. interfaceName(5)
- 6. agentCircuitId(6)
- 7. local(7)

portID: идентификатор порта.

deviceClass: Тип устройства LLDP-MED.

---

Описание события: Обнаружен конфликтный тип устройства LLDP-MED. Уведомление

Сообщение журнала: Обнаружен конфликт типа устройства LLDP-MED (на порту <portNum>, идентификатор шасси: <chassisType>, <chassisID>, идентификатор порта: <portType>, <portID>, класс устройства: <deviceClass>)

Параметры Описание:

portNum: Номер порта.

chassisType: chassis ID subtype.

Список значений:

- 1. chassisComponent(1) 2. interfaceAlias(2)
- 3. portComponent(3)
- 4. macAddress(4)
- 5. networkAddress(5)
- 6. interfaceName(6)
- 7. local(7)

chassisID: chassis ID subtype. portType: port ID subtype.

Список значений:

- 1. interfaceAlias(1)
- 2. portComponent(2)
- 3. macAddress(3)
- 4. networkAddress(4)
- 5. interfaceName(5)
- 6. agentCircuitId(6)
- 7. local(7)

portID: идентификатор порта.

deviceClass: Тип устройства LLDP-MED.

---

Описание события: Обнаружен несовместимый набор TLV LLDP-MED. Уведомление

---

---

Сообщение журнала: Обнаружен несовместимый набор LLDAP-MED TLV (на порту <portNum>, идентификатор шасси: <chassisType>, <chassisID>, идентификатор порта: <portType>, <portID>, класс устройства: <deviceClass>)

Параметры Описание:

portNum: Номер порта.

chassisType: chassis ID subtype.

Список значений:

1. chassisComponent(1)
2. interfaceAlias(2)
3. portComponent(3)
4. macAddress(4)
5. networkAddress(5)
6. interfaceName(6)
7. local(7)

chassisID: ичassis ID. portType: port ID subtype

Список значений:

1. interfaceAlias(1)
2. portComponent(2)
3. macAddress(3)
4. networkAddress(4)
5. interfaceName(5)
6. agentCircuitId(6)
7. local(7)

portID: идентификатор порта.

deviceClass: Тип устройства LLDAP-MED.

---

## Login/Logout

Описание записей журнала	Уровень
<p>Описание события: Вход в систему через консоль успешно выполнен.</p> <p>Сообщение в журнале: Успешный вход в систему через консоль (имя пользователя: &lt;username&gt;) Параметры Описание:</p> <p>имя пользователя: Представляет текущего пользователя для входа в систему.</p>	Информационный
<p>Описание события: Неудачный вход в систему через консоль.</p> <p>Сообщение в журнале: Вход через консоль не удался (имя пользователя: &lt;имя пользователя&gt;) Параметры Описание:</p> <p>имя пользователя: Представляет текущего пользователя для входа в систему.</p>	Предупреждение
<p>Описание события: Консольный сеанс завершен по таймеру.</p> <p>Сообщение в журнале: Console session timed out (Username: &lt;username&gt;) Parameters Description:</p> <p>имя пользователя: Представляет текущего пользователя для входа в систему.</p>	Информационный

---

<p>Описание события: Выход из системы через консоль.</p> <p>Сообщение журнала: Выход из системы через консоль (имя пользователя: &lt;имя пользователя&gt;) Параметры Описание: имя пользователя: Представляет текущего пользователя входа в систему.</p>	Информационный
<p>Описание события: Вход в систему через Telnet успешно выполнен.</p> <p>Сообщение в журнале: Успешный вход в систему через Telnet (Имя пользователя: &lt;username&gt;, IP: &lt;ipaddr&gt;) Параметры Описание: имя пользователя: Представляет текущего пользователя входа в систему. ipaddr: IP-адрес клиента.</p>	Информационный
<p>Описание события: Неудачный вход в систему через Telnet.</p> <p>Сообщение журнала: Неудачный вход в систему через Telnet (Имя пользователя: &lt;username&gt;, IP: &lt;ipaddr&gt;) Параметры Описание: имя пользователя: Представляет текущего пользователя входа в систему. ipaddr: Представляет IP-адрес клиента.</p>	Предупреждение
<p>Описание события: Сессия Telnet завершилась по таймеру.</p> <p>Сообщение журнала: Telnet session timed out (Username: &lt;username&gt;, IP: &lt;ipaddr&gt;) Parameters Description: имя пользователя: Представляет текущего пользователя входа в систему. ipaddr: Представляет IP-адрес клиента.</p>	Информационный
<p>Описание события: Выход из системы через Telnet.</p> <p>Сообщение журнала: Выход из системы через Telnet (имя пользователя: &lt;username&gt;, IP: &lt;ipaddr&gt;) Параметры Описание: имя пользователя: Представляет текущего пользователя входа в систему. ipaddr: Представляет IP-адрес клиента.</p>	Информационный
<p>Описание события: Успешный вход в систему через SSH.</p> <p>Сообщение в журнале: Успешный вход через SSH (Имя пользователя: &lt;username&gt;, IP: &lt;ipaddr&gt;) Параметры Описание: имя пользователя: Представляет текущего пользователя входа в систему. ipaddr: IP-адрес клиента.</p>	Информационный
<p>Описание события: Неудачный вход в систему через SSH.</p> <p>Сообщение в журнале: Вход через SSH не удался (Имя пользователя: &lt;username&gt;, IP: &lt;ipaddr&gt;) Параметры Описание: имя пользователя: Представляет текущего пользователя входа в систему. ipaddr: Представляет IP-адрес клиента.</p>	Критический
<p>Описание события: Сессия SSH завершилась по таймеру.</p>	Информационный

Сообщение в журнале: SSH-сессия завершилась (имя пользователя: <username>, IP: <ipaddr>) Параметры  
Описание:

имя пользователя: Представляет текущего пользователя для входа в систему.

ipaddr: Представляет IP-адрес клиента.

Описание события: Выход из системы через SSH. Информационный

Сообщение журнала: Выход из системы через SSH (имя пользователя: <username>, IP: <ipaddr>) Параметры  
Описание:

имя пользователя: Представляет текущего пользователя входа в систему.

ipaddr: Представляет IP-адрес клиента.

## MSTP Debug Enhancement

Описание записей журнала	Уровень
<p>Описание события: Используется для записи события включения протокола Spanning Tree Protocol.</p> <p>Сообщение журнала: Протокол Spanning Tree включен</p>	Информационный
<p>Описание события: Используется для записи события, когда протокол Spanning Tree отключен.</p> <p>Сообщение журнала: Протокол Spanning Tree отключен</p>	Информационный
<p>Описание события: Используется для записи события изменения топологии экземпляра MSTP.</p> <p>Сообщение журнала: Topology changed (Instance : &lt;Instance-id&gt;, &lt;interface_id&gt;, MAC:&lt;macaddr&gt;)</p> <p>Параметры Описание: Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST. interface_id: Номер порта, который обнаруживает или получает информацию о топообмене. macaddr: mac-адрес системы моста.</p>	Уведомление
<p>Описание события: Используется для регистрации выбора нового корневого моста экземпляра MSTP.</p> <p>Сообщение журнала: [CIST   CIST Regional   MSTI Regional] New Root bridge selected ([Instance: &lt;Instance-id&gt;] MAC: &lt;macaddr&gt; Priority :&lt;priority&gt;)</p> <p>Параметры Описание: Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST. macaddr: mac-адрес системы моста. priority (приоритет): Значение приоритета моста должно быть кратно 4096.</p>	Информационный
<p>Описание события: Используется для регистрации выбора нового корневого порта экземпляра MSTP.</p> <p>Сообщение журнала: Выбран новый корневой порт (экземпляр:&lt;Instance-id&gt;, &lt;interface_id&gt;)</p>	Уведомление

<p>Параметры Описание:</p> <p>Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST.</p> <p>interface_id: Номер порта, который обнаруживает или получает информацию о топочанге.</p>	
<p>Описание события: Используется для записи события изменения состояния порта экземпляра MSTP.</p> <p>Log Message: Изменение состояния порта Spanning Tree (Instance :&lt;Instance-id&gt;, &lt;interface_id&gt;) &lt;old_status&gt; -&gt; &lt;new_status&gt;.</p> <p>Параметры Описание:</p> <p>Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST.</p> <p>interface_id: Номер порта, который обнаруживает или получает информацию о топочанге.</p> <p>old status: new status:</p> <p>Состояние STP порта. Значение может быть Disable, Discarding, Learning, Forwarding.</p>	Уведомление
<p>Описание события: Используется для записи события изменения роли порта экземпляра MSTP.</p> <p>Log Message: Spanning Tree port role change (Instance :&lt;Instance-id&gt;, &lt;interface_id&gt;) &lt;old_role&gt; -&gt; &lt;new_role&gt;</p> <p>Параметры Описание:</p> <p>Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST.</p> <p>Interface_id: Номер порта, который обнаруживает или получает информацию о топообмене.</p> <p>old role: new role :</p> <p>Роль port of stp. Значение может быть DisabledPort, AlternatePort, BackupPort, RootPort, DesignatedPort, MasterPort.</p>	Информационный
<p>Описание события: Используется для записи действия по созданию экземпляра MST.</p> <p>Log Message: Spanning Tree instance created (Instance :&lt;Instance-id&gt;) Parameters Description:</p> <p>Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST.</p>	Информационный
<p>Описание события: Используется для записи действия по удалению экземпляра MST.</p> <p>Log Message: Spanning Tree instance deleted (Instance :&lt;Instance-id&gt;) Parameters Description:</p> <p>Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST.</p>	Информационный
<p>Описание события: Используется для записи действия по изменению версии STP.</p> <p>Log Message: Изменение версии Spanning Tree (новая версия :&lt;new_version&gt;) Параметры Описание:</p> <p>new_version: Работает под какой версией STP.</p>	Информационный

<p>Описание события: Используется для записи измененного имени конфигурации и уровня ревизии в идентификаторе конфигурации MST.</p> <p>Сообщение журнала: Изменение имени и уровня ревизии идентификатора конфигурации MST Spanning Tree (имя: &lt;имя&gt;, уровень ревизии &lt;уровень_ревизии&gt;).</p> <p>Параметры Описание: name: Имя, заданное для указанного региона MST. уровень ревизии (revision_level): Коммутаторы с одинаковым именем, но с разным уровнем ревизии считаются членами разных регионов MST.</p>	Информационный
<p>Описание события: Используется для записи действий по сопоставлению VLAN(ов) с экземпляром MST.</p> <p>Сообщение журнала: Spanning Tree MST configuration ID VLAN mapping table change (instance: &lt;Instance-id&gt; add vlan &lt;startvlanid&gt; [- &lt;endvlanid&gt;]).</p> <p>Параметры Описание: Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST. startvlanid: Начальный vid диапазона add vlan. endvlanid: Конечный vid диапазона add vlan.</p>	Информационный
<p>Описание события: Используется для записи действия по удалению VLAN(ов) из экземпляра MST.</p> <p>Сообщение журнала: Изменение таблицы отображения VLAN в конфигурации MST (экземпляр: &lt;Instance-id&gt; delete vlan &lt;startvlanid&gt; [- &lt;endvlanid&gt;]).</p> <p>Параметры Описание: Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST. startvlanid: Начальный vid удаляемого диапазона vlan. endvlanid: Конечный vid удаляемого диапазона vlan.</p>	Информационный
<p>Описание события: Используется для записи события, когда роль порта изменилась на альтернативную из-за guard root.</p> <p>Log Message: Изменение роли порта Spanning Tree (Instance :&lt;instance-id&gt;, &lt;interface-id&gt;) на альтернативный порт из-за корня guard.</p> <p>Параметры Описание: Instance-id: Идентификатор экземпляра MST. Instance 0 представляет экземпляр по умолчанию, CIST. Interface_id: Номер порта, который обнаружил событие.</p>	Информационный

## Peripheral

Описание записей журнала	Уровень
<p>Описание события: Вентилятор восстановлен.</p> <p>Сообщение журнала: &lt;fan-descr&gt; возврат к норме Описание параметров: fan-descr: Идентификатор вентилятора и его положение.</p>	Критический



<p>Описание события: Сбой вентилятора.</p> <p>Сообщение журнала: &lt;fan-descr&gt; failed</p> <p>Параметры Описание: fan-descr: Идентификатор вентилятора и его положение.</p>	Критический
<p>Описание события: Датчик температуры переходит в состояние тревоги.</p> <p>Сообщение журнала: &lt;тепловой датчик-descr&gt; обнаруживает аномальную температуру &lt;градус&gt; Параметры Описание: thermal-sensor-descr: Идентификатор датчика и его положение. градус: Текущая температура.</p>	Критический
<p>Описание события: Температура восстанавливается до нормы.</p> <p>Сообщение в журнале: &lt;термодатчик-descr&gt; температура вернулась к норме Параметры Описание: thermal-sensor-descr: Идентификатор датчика и его положение.</p>	Критический
<p>Описание события: Отказ питания.</p> <p>Сообщение журнала: &lt;power-descr&gt; failed Параметры Описание: power-descr: Положение и идентификатор питания.</p>	Критический
<p>Описание события: Питание восстановлено.</p> <p>Сообщение в журнале: &lt;power-descr&gt; возврат к норме Параметры Описание: power-descr: Положение и идентификатор питания.</p>	Критический
<p>Описание события: Нажмите кнопку сброса к заводским настройкам.</p> <p>Сообщение журнала: Нажата кнопка сброса к заводским настройкам</p>	Критический

## РоЕ

Описание записей журнала	Уровень
<p>Описание события: Превышен порог общего энергопотребления. Сообщение в журнале: Превышен порог использования &lt;процент&gt; Параметры Описание: процент: Порог использования.</p>	Предупреждение
<p>Описание события: Восстановлен порог использования общей мощности. Сообщение в журнале: Восстановлен порог использования &lt;процент&gt; Параметры Описание: процент: Порог использования.</p>	Предупреждение
<p>Описание события: PD не отвечает на запрос ping.</p> <p>Сообщение журнала: ASV: проверка живого состояния PD не удалась. (Порт: &lt;portNum&gt;, PD: &lt;ipaddr&gt;) Параметры Описание: portNum: Номер порта. ipaddr: IP-адрес PD.</p>	Предупреждение

## Port Security

Описание записей журнала	Уровень
<p>Описание события: Заполнен адрес на порту.</p> <p>Сообщение журнала: MAC-адрес &lt;macaddr&gt; вызывает нарушение безопасности порта на &lt;interface-id&gt;.</p> <p>Параметры Описание: macaddr: MAC-адрес нарушения. interface-id: Имя интерфейса.</p>	Предупреждение
<p>Описание события: Адрес в системе заполнен.</p> <p>Сообщение журнала: Превышен лимит на количество записей в системе</p>	Предупреждение

## Safeguard

Описание записей журнала	Уровень
<p>Описание события: Хост переходит в режим истощения.</p> <p>Сообщение журнала: Safeguard Engine входит в режим EXHAUSTED</p>	Предупреждение
<p>Описание события: Хост переходит в нормальный режим.</p> <p>Сообщение журнала: Safeguard Engine переходит в НОРМАЛЬНЫЙ режим</p>	Информационный

## SNMP

Описание записей журнала	Уровень
<p>Описание события: Получен SNMP-запрос с недопустимой строкой сообщества.</p> <p>Сообщение журнала: SNMP-запрос получен от &lt;ipaddr&gt; с недопустимой строкой сообщества Параметры Описание: ipaddr: IP-адрес.</p>	Информационный

## SSH

Описание записей журнала	Уровень
<p>Описание события: Сервер SSH включен.</p> <p>Сообщение журнала: SSH-сервер включен</p>	Информационный
<p>Описание события: SSH-сервер отключен.</p> <p>Сообщение журнала: SSH-сервер отключен</p>	Информационный

## Storm Control

Описание записей журнала	Уровень
<p>Описание события: Возникновение шторма.</p> <p>Log Message: &lt;Broadcast   Multicast   Unicast&gt; storm is occurring on &lt;interface-id&gt;.</p> <p>Параметры Описание: Broadcast: Шторм вызван ширококестельными пакетами (DA</p>	Предупреждение

---

= FF:FF:FF:FF:FF:FF:FF:FF).

Multicast: Шторм вызван многоадресными пакетами, включая неизвестные L2 multicast, известные L2 multicast, неизвестные IP multicast и известные IP multicast.

Одноадресная передача: Шторм вызван одноадресными пакетами, включая известные и неизвестные одноадресные пакеты.

interface-id: Идентификатор интерфейса, на котором происходит шторм.

---

Описание события: Шторм устранен.

Информационный

Сообщение журнала: <Broadcast | Multicast | Unicast> шторм очищен на <interface-id> Параметры Описание:

Broadcast: Широковещательный шторм очищен.

Multicast: Многоадресный шторм устранен.

Одноадресный: Одноадресный шторм (включая как известные, так и неизвестные одноадресные пакеты) очищается.

interface-id: Идентификатор интерфейса, на котором устраняется шторм.

---

Описание события: Порт отключен из-за пакетного шторма.

Предупреждение

Сообщение журнала: <Интерфейс-id> в настоящее время отключен из-за шторма <Broadcast | Multicast | Unicast>.

Описание параметров:

interface-id: Идентификатор интерфейса, на котором происходит отключение из-за шторма.

Broadcast: Интерфейс отключен из-за широковещательного шторма.

Multicast: Интерфейс отключен многоадресным штормом.

Одноадресная передача: Интерфейс отключен одноадресным штормом (включая как известные, так и неизвестные одноадресные пакеты).

---

## System

Описание записей журнала	Уровень
Описание события: Этот журнал будет создан при теплом запуске системы. Сообщение журнала: Теплый запуск системы	Критический
Описание события: Этот журнал генерируется при холодном запуске системы. Сообщение журнала: Холодный запуск системы	Критический
Описание события: Этот журнал генерируется при запуске системы. Сообщение журнала: Система запущена	Критический

## Telnet

Описание записей журнала	Уровень
Описание события: Успешный вход в систему через Telnet.	Информационный

<p>Сообщение в журнале: Успешный вход в систему через Telnet (Имя пользователя: &lt;username&gt;, IP: &lt;ipaddr&gt;) Параметры</p> <p>Описание:</p> <p>ipaddr: IP-адрес клиента Telnet.</p> <p>Имя пользователя: Имя пользователя, используемое для входа на сервер Telnet.</p>	
<p>Описание события: Не удалось войти в систему через Telnet.</p> <p>Сообщение журнала: Login failed through Telnet (Username: &lt;username&gt;, IP: &lt;ipaddr&gt;) Parameters Description:</p> <p>ipaddr: IP-адрес клиента Telnet.</p> <p>Имя пользователя: Имя пользователя, которое использовалось для входа на сервер Telnet.</p>	Предупреждение
<p>Описание события: Выход из системы через Telnet.</p> <p>Сообщение журнала: Выход из системы через Telnet (Имя пользователя: &lt;username&gt;, IP: &lt;ipaddr&gt;) Параметры</p> <p>Описание:</p> <p>ipaddr: IP-адрес клиента Telnet.</p> <p>Имя пользователя: Имя пользователя, которое используется для входа на сервер Telnet.</p>	Информационный
<p>Описание события: Сессия Telnet завершилась по таймеру.</p> <p>Сообщение журнала: Telnet session timed out (Username: &lt;username&gt;, IP: &lt;ipaddr&gt;) Parameters Description:</p> <p>ipaddr: IP-адрес клиента Telnet.</p> <p>Имя пользователя: Имя пользователя, используемое для входа на сервер Telnet.</p>	Информационный

## Voice-VLAN

Описание записей журнала	Уровень
<p>Описание события: При обнаружении нового голосового устройства на интерфейсе.</p> <p>Сообщение журнала: Обнаружено новое голосовое устройство (&lt;interface-id&gt;, MAC: &lt;mac-address&gt;) Параметры</p> <p>Описание:</p> <p>interface-id: Имя интерфейса.</p> <p>mac-адрес: MAC-адрес голосового устройства.</p>	Информационный
<p>Описание события: Когда интерфейс, находящийся в режиме автоматической голосовой сети VLAN, присоединяется к голосовой сети VLAN.</p> <p>Log Message: &lt;interface-id&gt; add into voice VLAN &lt;vid&gt;</p> <p>Параметры Описание:</p> <p>interface-id: Имя интерфейса.</p> <p>vid: идентификатор виртуальной локальной сети.</p>	Информационный
<p>Описание события: Когда интерфейс покидает голосовую VLAN и в то же время в интервале старения для этого интерфейса не обнаружено ни одного голосового устройства, будет отправлено сообщение журнала.</p>	Информационный

---

Сообщение журнала: <interface-id> remove from voice VLAN  
<vid> Описание параметров:  
interface-id: Имя интерфейса.  
vid: идентификатор виртуальной локальной сети.

---

## Web

Описание записей журнала	Уровень
<p>Описание события: Успешный вход в систему через Web. Сообщение журнала: Successful login through Web (Username: &lt;username&gt;, IP: &lt;ipaddr&gt;) Параметры Описание: username: Имя пользователя, которое используется для входа на HTTP-сервер. ipaddr: IP-адрес HTTP-клиента.</p>	Информационный
<p>Описание события: Не удалось войти в систему через Web. Сообщение журнала: Login failed through Web (Username: &lt;username&gt;, IP: &lt;ipaddr&gt;) Parameters Description: имя пользователя: Имя пользователя, которое используется для входа на HTTP-сервер. ipaddr: IP-адрес HTTP-клиента.</p>	Предупреждение
<p>Описание события: Веб-сессия завершилась по таймеру. Сообщение в журнале: Web-сессия завершилась (имя пользователя: &lt;username&gt;, IP: &lt;ipaddr&gt;) Параметры Описание: имя пользователя: Имя пользователя, используемое для входа на HTTP-сервер. ipaddr: IP-адрес HTTP-клиента.</p>	Информационный
<p>Описание события: Выход из системы через веб. Сообщение журнала: Logout through Web (Username: &lt;username&gt;, IP: &lt;ipaddr&gt;) Parameters Description: имя пользователя: Имя пользователя, которое используется для входа на HTTP-сервер. ipaddr: IP-адрес HTTP-клиента.</p>	Информационный
<p>Описание события: Успешный вход в систему через Web (SSL). Сообщение в журнале: Успешный вход в систему через Web (SSL) (имя пользователя: &lt;username&gt;, IP: &lt;ipaddr&gt;). Описание параметров: имя пользователя: имя пользователя, используемое для входа на сервер SSL. ipaddr: IP-адрес клиента SSL.</p>	Информационный
<p>Описание события: Не удалось войти в систему через Web (SSL). Сообщение в журнале: Login failed through Web (SSL) (Username: &lt;username&gt;, IP: &lt;ipaddr&gt;) Parameters Description: имя пользователя: имя пользователя, которое использовалось для входа на сервер SSL. ipaddr: IP-адрес клиента SSL.</p>	Предупреждение
<p>Описание события: Веб-сессия (SSL) завершилась по таймеру.</p>	Информационный

---

Сообщение в журнале: Web (SSL) session timed out (Username:  
<username>, IP: <ipaddr>) Parameters Description:

имя пользователя: имя пользователя, используемое для  
входа на сервер SSL.

ipaddr: IP-адрес клиента SSL.

---

Описание события: Выход из системы через веб (SSL).

Информационный

Сообщение журнала: Logout through Web (SSL) (Username:  
<username>, IP: <ipaddr>) Parameters Description:

имя пользователя: имя пользователя, которое используется  
для входа на сервер SSL.

ipaddr: IP-адрес клиента SSL.

---

## Приложение Б. Записи trap-сообщений

В следующей таблице перечислены все возможные записи trap-сообщений и их соответствующие значения, которые появятся в коммутаторе.

### 802.1X

Сообщение trap	Описание	OID
dDot1xExtLoggedSuccess	Хост прошел аутентификацию 802.1X. Вариабельные привязки: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName	1.3.6.1.4.1.171 .11.165.1000.3 0.0.1
dDot1xExtLoggedFail	Хост не прошел аутентификацию 802.1X. Вариабельные привязки: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName (5) dDot1xExtNotifyFailReason	1.3.6.1.4.1.171 .11.165.1000.3 0.0.2

### Authentication Fail

Сообщение trap	Описание	OID
authenticationFailure	SNMPv2-устройство в роли агента получило сообщение протокола, которое не аутентифицировано должным образом. Данное trap-сообщение генерируется всеми реализациями SNMPv2 и будет отправлено, только если параметр snmpEnableAuthenTraps включен.	1.3.6.1.6.3.1.1. 5.5

### DHCP Server Screen Prevention

Сообщение trap	Описание	OID
dDhcpFilterAttackDetected	Если функция DHCP Server Screen включена, trap-сообщения будут отправлены при получении каждого пакета ложного DHCP-сервера. Вариабельные привязки:	1.3.6.1.4.1.171 .11.165.1000.1 33.0.1

- 
- (1) dDhcpFilterLogBufServerIpAddr
  - (2) dDhcpFilterLogBufClientMacAddr
  - (3) dDhcpFilterLogBufferVlanId
  - (4) dDhcpFilterLogBufferOccurTime
- 

## DoS Prevention

Сообщение trap	Описание	OID
dDosPreveAttackDetectedPacket	Обнаружена DoS-атака. Вариабельные привязки: (1) dDoSPrevCtrlAttackType (2) dDosPrevNotiInfoDropIpAddr (3) dDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.171 .11.165.1000.5 9.0.2

## ErrDisable

Сообщение trap	Описание	OID
dErrDisNotifyPortDisabledAssert	Порт перешел в состояние Error-Disabled. Вариабельные привязки: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171 .11.165.1000.4 5.0.1
dErrDisNotifyPortDisabledClear	Порт возвращается в исходное состояние по истечению определенного интервала времени. Вариабельные привязки: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171 .11.165.1000.4 5.0.2

## General Management

Сообщение trap	Описание	OID
dGenMgmtLoginFail	Эта ловушка отправляется при неудачном входе пользователя в систему коммутатора. Объекты привязки: (1) dGenMgmtNotifyInfoLoginType (2) dGenMgmtNotifyInfoUserName	1.3.6.1.4.1.171 .11.165.1000.1 65.0.1

## Gratuitous ARP

Сообщение trap	Описание	OID
agentGratuitousARPTrap	Обнаружен конфликт IP-адреса. Вариабельные привязки: (1) ipaddr (2) macaddr	1.3.6.1.4.1.171 .11.165.1000.7 5.0.1



- 
- (3) portNumber
  - (4) agentGratuitousARPIInterfaceName
- 

## IMPB

Сообщение trap	Описание	OID
dImpbViolationTrap	Уведомление о нарушении адреса генерируется при обнаружении нарушения адреса привязки IP-MAC-Port. Объекты привязки: (1) ifIndex (2) dImpbViolationIpAddrType (3) dImpbViolationIpAddress (4) dImpbViolationMacAddress	1.3.6.1.4.1.171 .11.165.1000.2 2.0.1

## LACP

Сообщение trap	Описание	OID
linkUp	SNMP-устройство в роли агента обнаружило, что один из каналов связи перешел из состояния «down» в какое-то другое состояние (за исключением состояния notPresent). Текущее состояние указано в привязке ifOperStatus. Вариабельные привязки: (1) ifIndex, (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1 .5.4
linkDown	SNMP-устройство в роли агента обнаружило, что один из каналов связи перешел в состояние «down» из какого-то другого состояния (за исключением состояния notPresent). Предыдущее состояние указано в привязке ifOperStatus. Вариабельные привязки: (1) ifIndex, (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1 .5.3

## LBD

Сообщение trap	Описание	OID
dLbdLoopOccurred	Обнаружена петля. Вариабельные привязки: (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171 .11.165.1000.4 6.0.1

dLbdLoopRestart	Порт возвращается в исходное состояние по истечению определенного интервала времени. Варибельные привязки: (1) dLbdNotifyInfoIndex	1.3.6.1.4.1.171 .11.165.1000.4 6.0.2
dLbdVlanLoopOccurred	Обнаружена петля в режиме LBD VLAN-Based. Варибельные привязки: (1) dLbdNotifyInfoIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171 .11.165.1000.4 6.0.3
dLbdVlanLoopRestart	Порт возвращается в исходное состояние в режиме LBD VLAN-based по истечению определенного интервала времени. Варибельные привязки: (1) dLbdNotifyInfoIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171 .11.165.1000.4 6.0.4

## LLDP-MED

Сообщение trap	Описание	OID
lldpRemTablesChange	Значение lldpStatsRemTableLastChangeTime изменилось. Варибельные привязки: (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.0.8802.1.1.2 .0.0.1
lldpXMedTopologyChangeDetected	Обнаружено изменение в топологии: к порту было подключено новое устройство, удаленное устройство было отключено или было отключено с дальнейшим подключением к другому порту. Варибельные привязки: (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass	1.0.8808.1.1.2 .1.5.4795.0.1

## MAC Notification

Сообщение trap	Описание	OID
dL2FdbMacNotification	Изменение MAC-адресов в таблице коммутации. Варибельные привязки: (1) dL2FdbMac ChangeNotifyInfo	1.3.6.1.4.1.171 .11.165.1000.3 .0.1

## MSTP

Сообщение trap	Описание	OID
newRoot	Новый корень Spanning Tree. Trap-сообщение будет отправлено мостом сразу же после его назначения в качестве нового корня. По истечении таймера (Topology Change Timer) мост немедленно будет назначен корнем. Отправка данного trap-сообщения является опциональной.	1.3.6.1.2.1.17. 0.1
topologyChange	Мост отправляет trap-сообщение, когда какой-то из его настроенных портов переходит из состояния Learning в состояние Forwarding или из состояния Forwarding в состояние Blocking. Данное trap-сообщение не отправляется повторно. Отправка данного trap-сообщения является опциональной.	1.3.6.1.2.1.17. 0.2

## Peripheral

Сообщение trap	Описание	OID
dEntityExtFanStatusChg	Уведомление об изменении статуса вентилятора. Связующие объекты: (1) dEntityExtEnvFanIndex (2) dEntityExtEnvFanStatus	1.3.6.1.4.1.171 .11.165.1000.5 .0.1
dEntityExtThermalStatusChg	Уведомление об изменении состояния температуры. Связующие объекты: (1) dEntityExtEnvTempUnitId (2) dEntityExtEnvTempIndex (3) dEntityExtEnvTempStatus	1.3.6.1.4.1.171 .11.165.1000.5 .0.2
dEntityExtFactoryResetButton	Нажмите кнопку сброса к заводским настройкам. (1) dEntityExtUnitIndex	1.3.6.1.4.1.171 .11.165.1000.5 .0.5

## PD Alive

Сообщение trap	Описание	OID
dPoelfPdAliveFailOccurNotification	Эта ловушка показывает, ответил ли PD на запрос ping. Между уведомлениями, испускаемыми одним и тем же экземпляром объекта, должно пройти не менее 500 мс. Связывающие объекты: (1) pethMainPseGroupIndex (2) pethPsePortIndex (3) dPoelfPdAliveCfgPdIpType (4) dPoelfPdAliveCfgPdIpAddr	1.3.6.1.4.1.171 .14.24.0.4

**PoE**

Сообщение trap	Описание	OID
pethMainPowerUsageOnNotification	Эта ловушка указывает на включение индикации использования PSE Threshold, мощность использования выше порога. Между уведомлениями, испускаемыми одним и тем же экземпляром объекта, должно пройти не менее 500 мс. Связываемые объекты: (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105 .0.2
pethMainPowerUsageOffNotification	Эта ловушка указывает на то, что индикация использования PSE Threshold выключена, мощность использования ниже порогового значения. Между уведомлениями, испускаемыми одним и тем же экземпляром объекта, должно пройти не менее 500 мс. Связываемые объекты: (1) pethMainPseConsumptionPower	1.3.6.1.2.1.10 5.0.3
dPoelfPowerDeniedNotification	Это уведомление указывает, если диаграмма состояния PSE переходит в состояние POWER_DENIED. Между уведомлениями, испускаемыми одним и тем же экземпляром объекта, должно пройти не менее 500 мс. Связываемые объекты: (1) pethPsePortPowerDeniedCounter	1.3.6.1.4.1.17 1.14.24.0.1
dPoelfPowerOverLoadNotification	Эта ловушка указывает, если диаграмма состояния PSE переходит в состояние ERROR_DELAY_OVER. Между уведомлениями, испускаемыми одним и тем же экземпляром объекта, должно пройти не менее 500 мс. Связываемые объекты: (1) pethPsePortOverLoadCounter	1.3.6.1.4.1.17 1.14.24.0.2
dPoelfPowerShortCircuitNotification	Эта ловушка указывает, если диаграмма состояния PSE переходит в состояние ERROR_DELAY_SHORT. Между уведомлениями, испускаемыми одним и тем же экземпляром объекта, должно пройти не менее 500 мс. Связываемые объекты: (1) pethPsePortShortCounter	1.3.6.1.4.1.17 1.14.24.0.3

**Port**

Сообщение trap	Описание	OID
linkUp	При соединении портов генерируется уведомление. Объекты привязки:	1.3.6.1.6.3.1.

	(1) ifIndex (2) if AdminStatus (3) ifOperStatus	1.5.4
linkDown	При отключении порта генерируется уведомление. Объекты привязки: (1) ifIndex (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1. 1.5.3

## Port Security

Сообщение trap	Описание	OID
dPortSecMacAddrViolation	Если отправка trap-сообщений Port Security включена, trap-сообщения будут отправлены при обнаружении недопустимых MAC-адресов. Вариабельные привязки: (1) ifIndex, (2) dPortSecIfCurrentStatus (3) dPortSecIfViolationMacAddress	1.3.6.1.4.1.171.11.165.1000.8.0.1

## RMON

Сообщение trap	Описание	OID
risingAlarm	Запись уровня alarm превысила заданный верхний порог. Вариабельные привязки: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16. 0.1
fallingAlarm	Запись уровня alarm снизилась до заданного нижнего порога. Вариабельные привязки: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16. 0.2

## Safeguard

Сообщение trap	Описание	OID
dSafeguardChgToExhausted	Нормальный режим работы системы	1.3.6.1.4.1.171.11.165.1000.1

	изменился на режим высокой загрузки. Вариабельные привязки: (1) dSafeguardEngineCurrentMode	9.1.1.0.1
dSafeguardChgToNormal	Режим высокой загрузки системы изменился на нормальный режим. Вариабельные привязки: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.171 .11.165.1000.1 9.1.1.0.2

## Start

Сообщение trap	Описание	OID
coldStart	Повторная инициализация SNMPv2-устройства в роли агента и возможное изменение его настроек.	1.3.6.1.6.3.1.1 .5.1
warmStart	Повторная инициализация SNMPv2-устройства в роли агента с неизменной конфигурацией.	1.3.6.1.4.1.17 1.14.9.0.2

## System File

Сообщение trap	Описание	OID
dsfUploadImage	Пользователь успешно выгрузил файл образа.	1.3.6.1.4.1.171 .11.165.1000.1 4.0.1
dsfDownloadImage	Пользователь успешно загрузил файл образа.	1.3.6.1.4.1.171 .11.165.1000.1 4.0.2
dsfUploadCfg	Пользователь успешно выгрузил конфигурационный файл.	1.3.6.1.4.1.171 .11.165.1000.1 4.0.3
dsfDownloadCfg	Пользователь успешно загрузил конфигурационный файл.	1.3.6.1.4.1.171 .11.165.1000.1 4.0.4
dsfSaveCfg	Пользователь успешно сохранил конфигурационный файл.	1.3.6.1.4.1.171 .11.165.1000.1 4.0.5

## Storm Control

Сообщение trap	Описание	OID
dStormCtrlOccurred	Эта ловушка отправляется, когда dStormCtrlNotifyEnable имеет значение 'stormOccurred' или 'both' и обнаружен шторм. Объекты привязки: (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171 .11.165.1000.2 5.0.1
dStormCtrlStormCleared	Эта ловушка отправляется, когда dStormCtrlNotifyEnable имеет значение 'stormCleared' или 'both' и шторм очищен. Объекты привязки: (1) ifIndex	1.3.6.1.4.1.171 .11.165.1000.2 5.0.2

---

(2) dStormCtrlNotifyTrafficType

---

## Приложение В - Назначение атрибутов RADIUS

Назначение атрибутов RADIUS на коммутаторе используется в модуле 802.1X. Следующие описания объясняют тип VLAN RADIUS Attributes Assignment.

Чтобы назначить **VLAN** сервером RADIUS, на сервере RADIUS должны быть настроены соответствующие параметры. Чтобы использовать назначение VLAN, RFC 3580 определяет следующие атрибуты туннеля в пакетах RADIUS.

В таблице ниже приведены параметры для VLAN:

RADIUS Tunnel Attribute	Описание	Значение	Использование
Tunnel-Type	Этот атрибут указывает туннельный протокол, который нужно использовать в качестве инициатора или терминатора туннеля.	13 (VLAN)	Обязательно
Tunnel-Medium-Type	Атрибут указывает используемую транспортную Среду.	6 (802)	Обязательно
Tunnel-Private-Group-ID	Атрибут указывает групповой ID для определенной туннельной сессии.	string	Обязательно

Краткое описание формата атрибута Tunnel-Private-Group-ID показано ниже.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Type      |      Length      |      Tag      |      String...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---

```

В таблице ниже приведено определение поля Tag (отличается от RFC 2868):

Значение поля Tag	Формат строки поля
0x01	Имя VLAN (ASCII)
0x02	VLAN ID (ASCII)
Другие (0x00, 0x03 ~ 0x1F, >0x1F)	При получении строки настройки VLAN коммутатор сначала будет проверять все существующие VLAN ID и выберет подходящий, который станет идентификатором данной VLAN. Если подходящий VLAN ID отсутствует, коммутатор



---

будет проверять доступные имена VLAN.

---

**Примечание:** поле тега больше 0x1F распознается как первый октет следующего поля.

Если пользователь сконфигурировал атрибут VLAN на RADIUS-сервере (например, VID 3) и аутентификация 802.1X, WAC или на основе MAC прошла успешно, порт будет назначен VLAN 3. Однако если пользователь не сконфигурировал атрибуты VLAN, порт, который не является членом Guest VLAN, будет храниться в текущей аутентификации VLAN, а порт, являющийся членом Guest VLAN, будет назначен в исходную VLAN.

## Приложение Г - Поддержка атрибутов IETF RADIUS

Для атрибутов RADIUS существуют определенные детали аутентификации, авторизации и конфигурации для запросов и ответов. В данном разделе приведен список атрибутов RADIUS, которые в данный момент поддерживает коммутатор.

Атрибуты RADIUS поддерживаются стандартом IETF и Vendor-Specific Attribute (VSA). VSA позволяет вендорам создавать собственные дополнительные атрибуты RADIUS. Для подробной информации о VSA D-Link обратитесь к **Приложению Г, «Поддержка атрибутов RADIUS»**.

Атрибуты RADIUS стандарта IETF определены в RFC 2865 Remote Authentication Dial-In User Service (RADIUS), RFC 2866 RADIUS Accounting, RFC 2868 RADIUS Attributes for Tunnel Protocol Support и RFC 2869 RADIUS Extensions.

Список атрибутов IETF RADIUS, поддерживаемых коммутатором Т-КОМ, приведен в таблице ниже.

### Атрибуты аутентификации RADIUS:

Номер	Атрибут IETF
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
12	Framed-MTU
18	Reply-Message
24	State
26	Vendor-Specific
27	Session-Timeout
29	Termination-Action
30	Called-Station-ID
31	Calling-Station-ID
32	NAS-Identifier
60	CHAP-Challenge
61	NAS-Port-Type
64	Tunnel-Type
65	Tunnel-Medium-Type
77	Connect-Info
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID
85	Acct-Interim-Interval
87	NAS-Port-ID

