



T-KOM
РОСАТОМ

Руководство пользователя (CLI)

Управляемые стекируемые коммутаторы T-KOM 3 уровня

Коммутаторы серии ТКК-313

Версия 1.00

Москва
2022

Содержание

Содержание	2
1. Введение.....	6
2. Базовые команды интерфейса командной строки.....	15
3. Команды 802.1X	33
4. Команды ACL (Список управления доступом).....	48
5. Команды управления доступом	79
6. Команды предотвращения атак ARP Spoofing	103
7. Команды Asymmetric VLAN	106
8. Команды Authentication, Authorization и Accounting(AAA)	107
9. Базовые команды настройки IPv4	136
10. Базовые команды настройки IPv6	147
11. Команды BPDU Protection	166
12. Команды Cable Diagnostics.....	170
13. Команды логирования выполненных команд	174
14. Команды Connectivity Fault Management (CFM).....	175
15. Команды CPU Access Control List (ACL)	223
16. Команды Debug.....	228
17. Команды DHCP Auto-Configuration	238
18. Команды DHCP Client.....	240
19. Команды DHCP Relay	244
20. Команды DHCP Server	275
21. Команды DHCP Server Screening	305
22. Команды DHCP Snooping	311
23. Команды DHCPv6 Client	327
24. Команды DHCPv6 Guard.....	331
25. Команды DHCPv6 Relay	336
26. Команды DHCPv6 Server.....	360
27. Команды Digital Diagnostics Monitoring (DDM).....	379
28. Команды клиента D-Link Discovery Protocol (DDP)	390
29. Команды D-Link Unidirectional Link Detection (DULD)	393

30. Команды Domain Name System (DNS).....	398
31. Команды предотвращения атак DoS.....	406
32. Команды Dynamic ARP Inspection	410
33. Команды Error Recovery	426
34. Команды Ethernet OAM.....	430
35. Команды Ethernet Ring Protection Switching (ERPS)	450
36. Команды File System.....	474
37. Команды Filter Database (FDB).....	482
38. Команды Filter NetBIOS	497
39. Команды GARP VLAN Registration Protocol (GVRP)	499
40. Команды Gratuitous ARP.....	509
41. Команды управления интерфейсом.....	513
42. Команды Internet Group Management Protocol(IGMP) Snooping.....	537
43. Команды L3 Control Packet Filtering.....	565
44. Команды IP Source Guard	567
45. Команды IP Utility	573
46. Команды IP-MAC-Port Binding (IMPB)	582
47. Команды IPv6 Snooping	586
48. Команды IPv6 Source Guard	591
49. Команды Jumbo Frame	599
50. Команды Layer 2 Protocol Tunnel (L2PT).....	600
51. Команды Link Aggregation Control Protocol (LACP)	609
52. Команды Link Layer Discovery Protocol (LLDP)	616
53. Команды Loopback Detection (LBD)	649
54. Команды аутентификации MAC.....	657
55. Команды Mirror	661
56. Команды Multicast Listener Discovery (MLD) Snooping.....	671
57. Команды Multicast VLAN	696
58. Команды Neighbor Discovery (ND) Inspection.....	708
59. Команды Network Access Authentication	713
60. Команды Network Load Balancing (NLB).....	728
61. Команды Network Time Protocol (NTP)	732
62. Команды Power over Ethernet (PoE)	748

63. Команды Policy-Based Routing (PBR)	758
64. Команды Port Security	761
65. Команды энергосбережения	769
66. Команды PPPoE Circuit-ID Tag Insertion.....	776
67. Команды Private VLAN	780
68. Команды Protocol Independent	787
69. Команды качества обслуживания (QOS)	800
70. Команды перезагрузки.....	838
71. Команды Remote Network MONitoring (RMON)	841
72. Команды Route Map.....	850
73. Команды Router Advertisement (RA) Guard	860
74. Команды Routing Information Protocol (RIP).....	864
75. Команды Routing Information Protocol NextGeneration (RIPng)	878
76. Команды Safeguard Engine.....	892
77. Команды сервера Secure File Transfer Protocol (SFTP).....	900
78. Команды Secure Shell (SSH).....	903
79. Команды Secure Sockets Layer (SSL).....	912
80. Команды sFlow	921
81. Команды Simple Mail Transfer Protocol (SMTP)	928
82. Команды протокола Simple Network ManagementProtocol (SNMP).....	934
83. Команды Single IP Management (SIM).....	957
84. Команды Spanning Tree Protocol (STP)	969
85. Команды стекирования	992
86. Команды Storm Control	999
87. Команды Super VLAN	1004
88. Команды Surveillance VLAN	1008
89. Команды портов коммутатора	1015
90. Команды управления системных файлов	1020
91. Команды System Log.....	1033
92. Команды времени и SNTP	1045
93. Команды временного диапазона	1052
94. Команды Traffic Segmentation	1055
95. Команды Virtual LAN (VLAN)	1058

96. Команды Virtual LAN (VLAN) Tunnel	1074
97. Команды Virtual Router Redundancy Protocol (VRRP)	1089
98. Команды Virtual Router Redundancy ProtocolVersion 3 (VRRPv3)	1098
99. Команды Voice VLAN	1107
100. Команды Web-аутентификации	1115
101. Команды Weighted Random Early Detection(WRED)	1121
Приложение А. Восстановление пароля (Password Recovery)	1127
Приложение Б. Записи системного журнала	1129
Приложение В. Записи trap-сообщений	1163
Приложение Г. Назначение атрибутов RADIUS	1177
Приложение Д. Поддержка атрибутов IETF RADIUS	1181

1. Введение

Описания команд в данном руководстве основаны на программном обеспечении версии 1.00. Перечисленный здесь список команд является подгруппой команд, поддерживаемых коммутаторами серии ТГК-313-24.

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

Руководство предназначено для сетевых администраторов и других IT-специалистов, использующих для управления коммутатором интерфейс командной строки (CLI). Это основной интерфейс управления коммутаторами серии ТГК-313-24. Настоящее руководство рассчитано на пользователей, знакомых с основными принципами работы Ethernet и организации современных локально-вычислительных сетей (ЛВС).

Условные обозначения

Условное обозначение	Описание
Полужирный шрифт	Команды, опции команд и ключевые слова. Ключевые слова в командной строке необходимо вводить именно так, как они отображены.
<i>КУРСИВ ЗАГЛАВНЫМИ</i>	Параметры или значения, которые необходимо указать. Параметры в командной строке необходимо заменить желаемыми.
Квадратные скобки []	Дополнительное значение или набор дополнительных аргументов
Фигурные скобки { }	Альтернативные ключевые слова, разделенные вертикальными линиями. Как правило, одно из ключевых слов в отдельных списках может быть выбрано.
Вертикальная линия	Дополнительные значения или аргументы заключаются в квадратные скобки и разделяются вертикальной линией. Как правило, одно или более значение или аргумент в отдельных списках может быть выбрано.
Голубой шрифт Courier	Экран консоли, включая примеры введенных команд с соответствующим выводом. Все примеры в данном руководстве основаны на коммутаторе ТГК-313-24/бд-М.

Предупреждения

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



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



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

предотвращения.



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

Описания команд

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

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

Режимы ввода команд

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

Интерфейс командной строки поддерживает пять уровней привилегий учетной записи пользователя:

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

В интерфейсе командной строки (CLI) доступно несколько режимов в следующем иерархическом порядке.

Базовые режимы:

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

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

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

- Пользователи с базовым уровнем привилегий **Basic user** осуществляют вход в режиме **User EXEC Mode**.
- Пользователи с расширенным уровнем доступа: **Advanced user, Power User, Operator** и **Administrator**, осуществляют вход в режиме **Privileged EXEC Mode**.

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

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

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

Доступные командные режимы и уровни привилегий:

Режим ввода команд / Уровень доступа	Описание
User EXEC Mode / Уровень Basic User	Самый низкий уровень приоритета среди пользовательских учетных записей. Доступ только к просмотру базовых настроек системы.
Privileged EXEC Mode / Уровень Advanced User	На данном уровне есть доступ к настройкам управления терминалом. Пользователь может получить доступ к просмотру ограниченной информации, не относящейся к безопасности.
Privileged EXEC Mode / Уровень Power User	Меньше команд, чем на уровне Operator. Доступны команды конфигурирования, за исключением команд уровня Operator и Administrator.
Privileged EXEC Mode / Уровень Operator	Изменение локальных и глобальных настроек терминала, контроль и выполнение некоторых задач администрирования. Исключен доступ к информации, относящейся к безопасности.
Privileged EXEC Mode / Уровень Administrator	Те же права, что и для уровня Operator, при этом пользователь также может просматривать и вносить изменения в настройки безопасности.

Global Configuration Mode / Уровень Operator	Применение глобальных настроек, за исключением настроек безопасности, для всей системы. Также используется для перехода к специальным режимам.
Global Configuration Mode / Уровень Administrator	Применение глобальных настроек для всей системы. Также используется для перехода к специальным режимам.
Interface Configuration Mode / Уровень Administrator	Режим настройки интерфейса
VLAN Interface Configuration Mode	Режим настройки интерфейса VLAN.

User EXEC Mode с базовым уровнем доступа Basic User

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

Privileged EXEC Mode с расширенным уровнем доступа Advanced User

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

Privileged EXEC Mode с уровнем доступа Power User

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

Privileged EXEC Mode с уровнем доступа Operator

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

Privileged EXEC Mode с уровнем доступа Administrator

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

Global Configuration Mode

Данный режим позволяет вносить изменения в глобальные настройки всей системы. Для входа в режим требуется учетная запись уровня Advanced User, Power User, Operator или Administrator. Настройки безопасности доступны только пользователям с учетной записью уровня Administrator. Помимо применения глобальных настроек для всей системы, данный режим также используется для перехода в специальные режимы конфигурирования. Для доступа к режиму глобальной конфигурации пользователь должен войти в систему с соответствующим уровнем учетной записи и ввести команду **configure terminal** в привилегированном режиме Privileged EXEC.

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

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

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

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

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

Interface Configuration Mode (Режим конфигурирования интерфейса)

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

VLAN Interface Configuration Mode (Режим конфигурирования интерфейса VLAN)

Режим конфигурирования интерфейсов VLAN используется для настройки параметров интерфейсов, назначенных VLAN.

Для доступа к режиму конфигурирования интерфейсов в VLAN необходимо использовать следующую команду в режиме глобальной конфигурации:

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

Создание пользовательской учетной записи

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

Рассмотрим следующий пример.

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

В данном примере мы получили доступ к команде `username`.

- В режиме User EXEC вводится команда **enable** для доступа к режиму Privileged EXEC.
- Далее используется команда **configure terminal** для перехода к глобальному режиму конфигурации. Данный режим позволяет использовать команду **username**.
- С помощью команды **username admin password admin** создается учетная запись пользователя с именем *admin* и паролем *admin*.
- Команда **username admin privilege 15** назначает 15-й уровень привилегий для учетной записи *admin*.
- Команда **line console** обеспечивает доступ к режиму конфигурации строки интерфейса.
- Команда **login local** объявляет коммутатору, что для получения доступа к консоли пользователю необходимо ввести учетные данные из локальной базы данных.

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

```
Switch# copy running-config startup-config
Destination filename startup-config? [y/n]: y
Saving all configurations to NV-RAM..... Done.
Switch#
```

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

```
DGS-3130-30TS Gigabit Ethernet Switch
Command Line Interface
Firmware: Build 1.00.001
Copyright (C) 2017 D-Link Corporation. All rights reserved.
User Access Verification
Username:admin
Password:*****
Switch#
```

Конфигурирование интерфейса

При конфигурировании физических портов коммутатора используется особое обозначение.

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

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

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

- Unit ID / Slot ID / ID порта

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

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

Сообщения об ошибке

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

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

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

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

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

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

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

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

Функции редактирования

Интерфейс командной строки коммутатора поддерживает следующие клавиши для редактирования.

Клавиша	Описание
---------	----------

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

Фильтрация результатов вывода команды **show**

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

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

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

```
Switch#show running-config | begin # DEVICE
# DEVICE
configure terminal
end

# AAA

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

Switch#
```

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

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

Switch#
```

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

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

Current configuration : 30689 bytes

#-----
#
#           DGS-3130-30TS Gigabit Ethernet Switch
#           Configuration
#
#           Firmware: Build 1.00.001
#           Copyright(C) 2017 D-Link Corporation. All rights reserved.
#-----

# STACK

end

# AAA

configure terminal
# AAA START
no aaa new-model
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.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

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

Пример

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

```
Switch#help

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

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

Switch#
```

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

```
Switch#re?
reboot          rename          renew          reset

Switch#re
```

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

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

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

2-2 enable

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

enable [PRIVILEGE-LEVEL]

Параметры

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

По умолчанию

Нет

Режим ввода командыUser EXEC Mode
Privileged EXEC Mode**Уровень команды по умолчанию**

Уровень 1

Использование команды

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

Пример

В данном примере показано изменение уровня привилегии активной сессии CLI на 15 уровень.

```
Switch# show privilege
Current privilege level is 2

Switch# enable 15
password:*****
Switch# show privilege
Current privilege level is 15

Switch#
```

2-3 disable

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

disable [PRIVILEGE-LEVEL]

Параметры

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

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

В данном примере показано изменение уровня привилегии активной сессии CLI на 1 уровень.

```
Switch# show privilege

Current privilege level is 15

Switch# disable 1
Switch> show privilege

Current privilege level is 1

Switch>
```

2-4 configure terminal

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

configure terminal

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для входа в режим глобальной конфигурации.

Пример

В данном примере показан процесс входа в режим глобальной конфигурации.

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

2-5 login (EXEC)

Данная команда используется для настройки имени пользователя.

login

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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

```
Switch# login
Username: user1
Password: xxxxx
Switch#
```

2-6 login (Line)

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

login [local] no login

Параметры

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

По умолчанию

По умолчанию для доступа через **консоль** учетные данные не заданы.
По умолчанию настроен метод входа для доступа по **Telnet** (с паролем).
По умолчанию настроен метод входа для доступа по **SSH** (с паролем).

Режим ввода команды

Line Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

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

Для доступа по SSH используется 3 типа аутентификации:

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

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

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

Пример

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

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

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

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

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

```
Switch#login
Password:*****
Switch#
```

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

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

В данном примере показан процесс конфигурации метода входа login local.

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

2-7 logout

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

logout

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

В данном примере показан процесс выхода из системы.

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

2-8 end

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

end

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode.
Любой режим конфигурации.

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

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

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

2-9 exit

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

exit

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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

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

2-10 show history

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

show history**Параметры**

Нет

По умолчанию

Нет

Режим ввода командыUser/Privileged EXEC Mode
Любой режим конфигурирования**Уровень команды по умолчанию**

Уровень 1

Использование команды

Все введенные команды сохраняются в системе. Для повторного вызова сохраненной команды используется сочетание клавиш CTRL+P или клавиша Вверх. В этом случае команды вызываются последовательно, начиная с последних команд. Буфер истории рассчитан на 20 команд.

Навигация по командам в истории выполняется следующими комбинациями клавиш:

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

Пример

В данном примере показан процесс вызова буфера истории.

```
Switch# show history
help
history
Switch#
```

2-11 password-recovery

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

password-recovery**Параметры**

Нет

По умолчанию

Нет

Режим ввода команды

Reset Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

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

Данная команда позволяет:

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

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

Пример

В данном примере показан процесс использования функции восстановления пароля.

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

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

Switch(reset-config)#
```

2-12 show environment

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

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

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

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

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

```
Switch#show environment

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

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

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

Switch#
```

Отображаемые параметры

Power Module	Power 1: питание переменным током (AC). Power 2: питание от резервного источника (RPS).
Power Status	in-operation: источник питания работает нормально. empty: источник питания не подключен.

2-13 show unit

Данная команда позволяет получить общую информацию о системе.

show unit [UNIT-ID]

Параметры

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

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

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

```
Switch#show unit

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

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

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

Switch#
```

2-14 show cpu utilization

Данная команда позволяет получить информацию об использовании CPU.

show cpu utilization

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

В данном примере показано получение информации о загрузке процессора.

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

2-15 show version

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

show version

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

В данном примере показано отображение информации о коммутаторе.

```
Switch#show version

System MAC Address: F0-7D-68-36-30-00

Unit ID      Module Name          Versions
-----
1           DGS-3130-30TS      H/W:A1
                                   Bootloader:1.00.001
                                   Runtime:1.00.001

Switch#
```

2-16 snmp-server enable traps environment

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

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

Параметры

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

По умолчанию

По умолчанию поддержка трапов для данных параметров отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

В данном примере показан процесс включения трапов.

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

2-17 environment temperature threshold

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

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

Параметры

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

По умолчанию

По умолчанию нормальным является тот же диапазон, что указан в рабочей температуре.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

В данном примере показан процесс настройки диапазона температуры для термосенсора ID 1 в устройстве Unit 1.

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

2-18 show privilege

Данная команда используется для отображения текущего уровня привилегий.

show privilege

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения текущего уровня привилегий.

Пример

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

```
Switch#show privilege
```

```
Current privilege level is 15
```

```
Switch#
```


3. Команды 802.1X

3-1 clear dot1x counters

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

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

Параметры

all	Обнуление счетчиков 802.1X (диагностика, статистика и статистика сессии) на всех интерфейсах.
interface INTERFACE-ID	Обнуление счетчиков 802.1X (диагностика, статистика и статистика сессии) на определенном интерфейсе. Допустимыми интерфейсами являются физические порты (включая тип, номер в стеке и номер порта).
,	(Опционально) Используется для перечисления отдельных интерфейсов и их групп. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

3-2 dot1x control-direction

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

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

Параметры

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

По умолчанию

По умолчанию используется двунаправленный режим.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

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

Пример

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

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

3-3 dot1x default

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

```
dot1x default
```

Параметры

Нет

По умолчанию

Аутентификация IEEE 802.1X отключена.
 Двухнаправленный режим потока.
 Управление портом автоматическое.
 Forward PDU на порту отключено.
 Максимум запросов – 2 раза.
 Таймер сервера – 30 секунд.
 Таймер запроса – 30 секунд.
 Интервал передачи – 30 секунд.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

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

По умолчанию

По умолчанию данная опция настроена как auto.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

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

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

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

Пример

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

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

3-5 dot1x forward-pdu

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

dot1x forward-pdu
no dot1x forward-pdu

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

3-6 dot1x initialize

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

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

Параметры

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

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

3-7 dot1x max-req

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

```
dot1x max-req TIMES
no dot1x max-req
```

Параметры

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

По умолчанию

По умолчанию используется значение 2

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

3-8 dot1x pae authenticator

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

dot1x pae authenticator
no dot1x pae authenticator

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

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

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

3-9 dot1x re-authenticate

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

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

Параметры

interface <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.
mac-address <i>MAC-ADDRESS</i>	Указание MAC-адреса для повторной аутентификации.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

3-11 dot1x timeout

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

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

Параметры

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

По умолчанию

Значение server-timeout по умолчанию составляет 30 секунд.
Значение supp-timeout по умолчанию составляет 30 секунд.
Значение tx-period по умолчанию составляет 30 секунд.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурации интерфейса физического порта.

Пример

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

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

3-12 show dot1x

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

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

Параметры

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

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

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

```
Switch#show dot1x

802.1X           : Enabled
Trap State       : Enabled

Switch#
```

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

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

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

Switch#
```

3-13 show dot1x diagnostics

Данная команда используется для просмотра результатов диагностики IEEE 802.1X.

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

Параметры

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

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

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

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

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

Switch#
```

3-14 show dot1x statistics

Данная команда используется для просмотра статистики IEEE 802.1X.

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

Параметры

interface *INTERFACE-ID* (Опционально) Интерфейс или группа интерфейсов, для которых будет

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

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

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

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

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

Switch#
```

3-15 show dot1x session-statistics

Данная команда используется для отображения статистики сессий IEEE 802.1X.

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

Параметры

interface <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

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

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

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

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

3-16 snmp-server enable traps dot1x

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

```
snmp-server enable traps dot1x
no snmp-server enable traps dot1x
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Нет

Пример

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

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

4. Команды ACL (Список управления доступом)

4-1 access-list resequence

Данная команда используется для того, чтобы 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

Уровень команды по умолчанию

Уровень 12

Использование команды

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

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

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

Пример

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

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

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

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

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

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

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

Switch(config)#
```

4-2 action

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

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

Параметры

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

По умолчанию

Параметр по умолчанию –forward.

Режим ввода команды

VLAN Access-map Sub-map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

4-3 expert access-group

Данная команда используется для применения указанных списков управления доступом expert (expert ACL) к интерфейсу. При использовании формы по команда отменит применение.

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

Параметры

<i>NAME</i>	Имя настраиваемого списка управления доступом expert (expert access-list). Максимальное число допустимых символов в имени – 32
<i>NUMBER</i>	Номер настраиваемого списка управления доступом expert (expert access-list).
in	(Опционально) Фильтрация входящих пакетов на интерфейс. Если направление не указано, используется значение in .
out	(Опционально) Фильтрация исходящих пакетов для

передачи интерфейсу.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

В данном примере показан процесс применения списка управления доступом expert к интерфейсу. Применяется ACL **exp_acl** на порту 1/0/2 для фильтрации входящих пакетов.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# expert access-group exp_acl in
Switch(config-if)# end
Switch# show access-group interface ethernet 1/0/2
eth1/0/2:
  Inbound expert access-list : exp_acl(ID: 8999)
Switch#
```

4-4 expert access-list

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

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

Параметры

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

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

```
Switch#configure terminal
Switch(config)#expert access-list extended exp_acl
Switch(config-exp-nacl)#
```

4-5 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} [in | out]
no ip access-group [NAME] [in | out]
```

Параметры

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

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

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

Пример

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

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

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

4-6 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
no ip access-list [extended] {NAME}
```

Параметры

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

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

4-7 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} [in | out]
no ipv6 access-group [NAME] [in | out]
```

Параметры

<i>NAME</i>	Укажите имя используемого списка доступа IPv6.
in	(Опционально) Указывает, что список доступа IPv6 будет применен для проверки пакетов во входящем направлении. Если направление не указано, используется in .
out	(Опционально) Указывает, что список доступа IPv6 будет применен для проверки пакетов в исходящем направлении.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

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

Пример

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

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

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

4-8 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
no ipv6 access-list [extended] {NAME}

Параметры

extended	(Опционально) Указывает, что список доступа IPv6 является расширенным списком доступа IPv6 и есть возможность применить больше опций фильтрации. Если параметр не указан, список доступа IPv6 будет считаться стандартным.
NAME	Назначаемое имя списка доступа IPv6. Максимальное число допустимых символов в имени – 32.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

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

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

4-9 mac access-group

Данная команда используется для применения списков управления доступом MAC (MAC access list) к интерфейсу. При использовании формы `no mac access-group` команда удалит группу доступа с интерфейса.

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

Параметры

<i>NAME</i>	Укажите имя используемого списка доступа MAC.
in	(Опционально) Указывает, что список доступа MAC будет применен для проверки пакетов во входящем направлении. Если параметр не указан, используется значение in .
out	(Опционально) Указывает, что список доступа MAC будет применен для проверки пакетов в исходящем направлении.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

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

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

Пример

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

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/4
Switch(config-if)#mac access-group daily-profile in

The remaining applicable MAC access entries are 896, 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. При использовании формы **no** команда удалит список доступа MAC.

```
mac access-list extended NAME
no mac access-list extended {NAME}
```

Параметры

<i>NAME</i>	Укажите имя списка управления доступом MAC (MAC access list). Максимально допустимая длина – 32 символа.
-------------	---

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы войти в режим MAC Access-List Configuration Mode, и введите команду **permit** или **deny**, чтобы указать записи. Указанное имя должно быть уникальным среди всех списков доступа. Имя чувствительно 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 match ip address

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

```
match ip address {ACL-NAME}
no match ip address
```

Параметры

<i>ACL-NAME</i>	Укажите имя списка управления доступом (ACL access list). Максимально допустимая длина – 32 символа.
-----------------	---

По умолчанию

Нет

Режим ввода команды

VLAN Access-map Sub-map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

VLAN access-map vlan-map 20
  match ip access list: spl(ID: 1999)
  action: forward

Switch#
```

4-12 match ipv6 address

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

```
match ipv6 address {ACL-NAME}
no match ipv6 address
```

Параметры

<i>ACL-NAME</i>	Укажите имя списка управления доступом IPv6 (IPv6 ACL). Максимально допустимая длина – 32 символа.
-----------------	---

По умолчанию

Нет

Режим ввода команды

VLAN Access-map Sub-map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

```

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

VLAN access-map vlan-map 20
  match ipv6 access list: spl(ID: 12999)
  action: forward

Switch#

```

4-13 match mac address

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

```

match mac address {ACL-NAME}
no match mac address

```

Параметры

<i>ACL-NAME</i>	Укажите имя списка управления доступом MAC (ACL MAC). Максимально допустимая длина – 32 символа.
-----------------	---

По умолчанию

Нет

Режим ввода команды

VLAN Access-map Sub-map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

VLAN access-map vlan-map 20
  match ip access list: spl(ID: 3999)
  action: forward
VLAN access-map vlan-map 30
  match mac access list: ext_mac(ID: 7999)
  action: forward

Switch#
```

4-14 permit | deny (expert access-list)

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

Расширенный список управления доступом Expert (Extended Expert ACL):

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

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

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

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

no SEQUENCE-NUMBER

Параметры

SEQUENCE-NUMBER

Укажите порядковый номер. Доступен диапазон от 1 до 65535 Чем меньше номер, тем выше приоритет правила permit/deny.

<i>PROTOCOL</i>	(Опционально) Укажите ID IP-протокола или одно из следующих имен протокола. Доступны следующие имена: eigrp, esp, gre, igmp, ospf, pim, vrrp, rsvp и ipinip. Если ID протокола указан, параметр MASK (0x0-0xff) является опциональным (необязательным). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
cos <i>OUTER-COS</i>	(Опционально) Укажите значение outer priority. Доступен диапазон значений от 0 до 7.
inner <i>INNER-COS</i>	(Опционально) Укажите значение внутреннего приоритета (inner priority). Доступен диапазон значений от 0 до 7.
vlan <i>OUTER-VLAN</i>	(Опционально) Укажите outer VLAN ID.
inner <i>INNER-VLAN</i>	(Опционально) Укажите inner VLAN ID.
any	Укажите для использования любого MAC-адреса источника, любого MAC-адреса назначения, любого IP-адреса источника или любого IP-адреса назначения.
host <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.
host <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.
host <i>SRC-IP-ADDR</i>	Укажите определенный IP-адрес узла источника.
<i>SRC-IP-ADDR SRC-IP-WILDCARD</i>	Укажите группу IP-адресов источника, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
host <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.
precedence <i>PRECEDENCE</i>	(Опционально) Укажите, чтобы пакеты могли фильтроваться по уровню приоритета (precedence). Доступны значения от 0 до 7
tos <i>TOS</i>	(Опционально) Укажите, чтобы пакеты могли фильтроваться по уровню type of service. Доступны значения от 0 до 15.
dscp <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 (по умолчанию) - 000000, ef - 101110

<i>lt</i> <i>PORT</i>	(Опционально) Укажите для сопоставления, если значение указанного порта меньше.
<i>gt</i> <i>PORT</i>	(Опционально) Укажите для сопоставления, если значение указанного порта больше.
<i>eq</i> <i>PORT</i>	(Опционально) Укажите для сопоставления, если значение указанного порта равно.
<i>neq</i> <i>PORT</i>	(Опционально) Укажите для сопоставления, если значение указанного порта не равно.
<i>range</i> <i>MIN-PORT MAX-PORT</i>	(Опционально) Укажите для сопоставления, если значение попадает в указанный диапазон портов.
<i>TCP-FLAG</i>	(Опционально) Укажите поля TCP flag и указанные биты заголовка TCP с именем ack (acknowledge), fin (finish), psh (push), rst (reset), syn (synchronize) или urg (urgent).
fragments	(Опционально) Укажите для фильтрации фрагментов пакета.
time-range <i>PROFILE-NAME</i>	(Опционально) Укажите имя профиля периода времени, связанного со списком доступа, определяющим период его активации.
<i>ICMP-TYPE</i>	(Опционально) Укажите тип сообщения ICMP. Доступны значения типа сообщений от 0 до 255
<i>ICMP-CODE</i>	(Опционально) Укажите код сообщения ICMP. Доступны значения кода сообщений от 0 до 255
<i>ICMP-MESSAGE</i>	(Опционально) Укажите сообщение ICMP. Для выбора доступны следующие предустановленные параметры: <i>beyond-scope</i> , <i>destination-unreachable</i> , <i>echo-reply</i> , <i>echo-request</i> , <i>header</i> , <i>hop-limit</i> , <i>mld-query</i> , <i>mld-reduction</i> , <i>mld-report</i> , <i>nd-na</i> , <i>nd-ns</i> , <i>next-header</i> , <i>no-admin</i> , <i>no-route</i> , <i>packet-too-big</i> , <i>parameter-option</i> , <i>parameter-problem</i> , <i>port-unreachable</i> , <i>reassembly-timeout</i> , <i>redirect</i> , <i>renum-command</i> , <i>renum-result</i> , <i>renum-seq-number</i> , <i>router-advertisement</i> , <i>router-renumbering</i> , <i>router-solicitation</i> , <i>time-exceeded</i> , <i>unreachable</i> .

По умолчанию

Нет

Режим ввода команды

Extended Expert Access-list Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

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

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

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

Если параметр **fragment** для параметров **tcp**, **udp** или **icmp** убран в команде **permit | deny (expert access-list)**, то пользователь все равно может использовать опцию **PROTOCOL** в команде **permit | deny (expert access-list)** для настройки параметра **fragment**.

Пример

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

```
Switch# configure terminal
Switch(config)# expert access-list extended exp_acl
Switch(config-exp-nacl)# deny tcp host 192.168.4.12 host 0013.0049.8272 any any
Switch(config-exp-nacl)#
```

4-15 permit | deny (ip access-list)

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

Расширенный список управления доступом (Extended Access List):

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

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

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

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


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

Стандартный список доступа IP (Standard IP Access List):

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

no SEQUENCE-NUMBER

Параметры

SEQUENCE-NUMBER	Укажите порядковый номер. Доступен диапазон от 1 до 65535 Чем меньше номер, тем выше приоритет правила permit/deny.
any	Укажите IP-адрес источника или IP-адрес назначения.
host SRC-IP-ADDR	Укажите определенный IP-адрес узла источника.
SRC-IP-ADDR SRC-IP-WILDCARD	Укажите группу IP-адресов источника, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
host DST-IP-ADDR	Укажите определенный IP-адрес узла назначения.
DST-IP-ADDR DST-IP-WILDCARD	Укажите группу IP-адресов назначения, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
precedence PRECEDENCE	(Опционально) Укажите, чтобы пакеты могли фильтроваться по уровню приоритета (precedence). Доступны значения от 0 до 7.
dscp DSCP	(Опционально) Укажите DSCP-код для совпадений с заголовком IP. Доступен диапазон от 0 до 63 или выбор из следующих имен DSCP: af11 - 001010, af12 - 001100, af13 - 001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 - 110000, cs7 - 111000, default (по умолчанию) - 000000, ef - 101110
tos TOS	(Опционально) Укажите, чтобы пакеты могли фильтроваться по уровню type of service. Доступны значения от 0 до 15
lt PORT	(Опционально) Укажите для сопоставления, если значение указанного порта меньше.
gt PORT	(Опционально) Укажите для сопоставления, если значение указанного порта больше.
eq PORT	(Опционально) Укажите для сопоставления, если значение указанного порта равно.
neq PORT	(Опционально) Укажите для сопоставления, если значение указанного порта не равно.
range MIN-PORT MAX-PORT	(Опционально) Укажите для сопоставления, если значение попадает в указанный диапазон портов.
time-range PROFILE-NAME	(Опционально) Укажите имя профиля периода времени, связанного

	со списком доступа, определяющим период его активации.
tcp, udp, igmp, gre, esp, eigrp, ospf, pcp, pim, vrrp	Укажите протоколы 4 уровня.
<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

Уровень команды по умолчанию

Уровень 12

Использование команды

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

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

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

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

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

Пример

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

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

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

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

4-16 permit | deny (ipv6 access-list)

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

Расширенный список доступа IPv6 (Extended IPv6 Access List):

[SEQUENCE-NUMBER] {**permit** | **deny**} **tcp** {**any** | **host** SRC-IPV6-ADDR | SRC-IPV6- ADDR/PREFIX-LENGTH} [{**eq** | **lt** | **gt** | **neq**} PORT | **range** MIN-PORT MAX-PORT] {**any** | **host** DST-IPV6-ADDR | DST-IPV6-ADDR/PREFIX-LENGTH} [{**eq** | **lt** | **gt** | **neq**} PORT | **range** MIN-PORT MAX-PORT][**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.
any	Укажите IPv6-адрес источника или IPv6-адрес назначения.
host <i>SRC-IPV6-ADDR</i>	Укажите определенный IPv6-адрес узла источника.
<i>SRC-IPV6-ADDR/PREFIX-LENGTH</i>	Укажите сеть IPv6 источника.
host <i>DST-IPV6-ADDR</i>	Укажите определенный IPv6-адрес узла назначения.
<i>DST-IPV6-ADDR/PREFIX-LENGTH</i>	Укажите сеть IPv6 назначения.
tcp, udp, icmp	Укажите тип протокола 4 уровня.
dscp <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 (по умолчанию) - 000000, ef - 101110
lt <i>PORT</i>	(Опционально) Укажите для сопоставления, если значение указанного порта меньше.
gt <i>PORT</i>	(Опционально) Укажите для сопоставления, если значение указанного порта больше.
eq <i>PORT</i>	(Опционально) Укажите для сопоставления, если значение указанного порта равно.
neq <i>PORT</i>	(Опционально) Укажите для сопоставления, если значение указанного порта не равно.
range <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: <i>beyond-scope</i> , <i>destination-unreachable</i> , <i>echo-reply</i> , <i>echo-request</i> , <i>erroneous_header</i> , <i>hop-limit</i> , <i>multicast-listener-query</i> , <i>multicast-listener-done</i> , <i>multicast-listener-report</i> , <i>nd-na</i> , <i>nd-ns</i> , <i>next-header</i> , <i>no-admin</i> , <i>no-route</i> , <i>packet-too-big</i> , <i>parameter-option</i> , <i>parameter-problem</i> , <i>port-unreachable</i> , <i>reassembly-timeout</i> , <i>redirect</i> , <i>renum-command</i> , <i>renum-result</i> , <i>renum-seq-number</i> , <i>router-advertisement</i> , <i>router-renumbering</i> , <i>router-solicitation</i> , <i>time-exceeded</i> , <i>unreachable</i> .
time-range <i>PROFILE-NAME</i>	(Опционально) Укажите имя профиля периода времени, связанного со списком доступа, определяющим период его активации.

По умолчанию

Нет

Режим ввода команды

IPv6 Access-list Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

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

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

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

Пример

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

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

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

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

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

Данная команда используется для определения правила для пакетов, которым будет разрешено или отказано в доступе. При использовании формы **no** команда удалит запись.

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

Параметры

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

vlan <i>VLAN-ID</i>	(Опционально) Укажите VLAN-ID.
inner <i>INNER-VLAN</i>	(Опционально) Укажите Inner VLAN ID.
time-range <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

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пользователь может использовать команду **access-list sequence** 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)# permit 00:80:33:00:00:00 00:00:00:ff:ff:ff any
Switch(config-mac-ext-acl)# permit 00:f4:57:00:00:00 00:00:00:ff:ff:ff any
Switch(config-mac-ext-acl)#
```

4-18 show access-group

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

show access-group [interface INTERFACE-ID]

Параметры

interface INTERFACE-ID	(Опционально) Укажите необходимые интерфейсы.
-------------------------------	---

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

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

```
Switch# show access-group

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

Switch#
```

4-19 show access-list

Данная команда используется для просмотра информации о настройках списка доступа.

show access-list [ip [NAME] | mac [NAME] | ipv6 [NAME]]

Параметры

ip	(Опционально) Укажите для отображения всех списков доступа IP.
mac	(Опционально) Укажите для отображения всех списков доступа.
ipv6	(Опционально) Укажите для отображения всех списков доступа IPv6.
NAME	(Опционально) Укажите имя списка доступа (access list), который необходимо отобразить.

По умолчанию

Нет

Режим ввода командыUser/Privileged EXEC Mode
Любой режим конфигурирования**Уровень команды по умолчанию**

Уровень 1

Использование команды

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
exp_acl(ID: 9999)                             expert ext-acl
ip6-control(ID: 14999)                       ipv6 ext-acl

Total Entries: 4

Switch#
```

В данном примере показано, как включить отображение списков доступа IP с именем Strict-Control.

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

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

Switch#
```

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

```
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: 12410 packets Egr: 85201 packets)
20 permit tcp any host 10.100.1.2 (Ing: 6532 packets Egr: 0 packets)
30 permit icmp any any (Ing: 8758 packets Egr: 4214 packets)

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

Switch#
```

4-20 show vlan access-map

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

show vlan access-map [MAP-NAME]

Параметры

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

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

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

```
Switch# show vlan access-map

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

Switch#
```

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

```
Switch# show vlan access-map

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

Switch#
```

4-21 show vlan filter

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

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

Параметры

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

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

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

```
Switch# show vlan filter

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

Switch#

Switch# show vlan filter vlan 5

VLAN ID 5
  VLAN Access Map: aa

Switch#
```

4-22 vlan access-map

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

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

Параметры

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

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

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

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

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

Пример

В данном примере показано, как создать VLAN access map.

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

4-23 vlan filter

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

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

Параметры

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

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

VLAN Map vlan-map
  Configured on VLANs: 5

Switch#
```

5. Команды управления доступом

5-1 access class

Данная команда используется для указания списка, которому необходимо ограничить доступ к сессии. Используйте форму **no**, чтобы отменить проверку указанного списка доступа.

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

Параметры

<i>IP-ACL</i>	Стандартный список доступа IP-адресов. Поле адреса источника с записью permit или deny определяет доверенный или недоверенный узел.
---------------	---

По умолчанию

Нет

Режим ввода команды

Line Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

5-2 banner login

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

banner login cMESSAGEc no banner login

Параметры

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

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

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



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

Пример

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

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

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


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

5-3 prompt

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

prompt *STRING*
no prompt

Параметры

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

По умолчанию

По умолчанию строка шифрует имя сервера SNMP.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет настроить подсказку командной строки. Если пользователь выберет шифрование имени сервера SNMP в качестве подсказки, зашифрованы будут только первые 15 символов. Подсказка может отобразить только 15 символов. Символ уровня привилегии будет отображаться последним символом подсказки.

Символы определяются по следующим правилам:

> – уровень пользователя

– уровень привилегии пользователя

Пример

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

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

5-4 enable password

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

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

Параметры

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

По умолчанию

По умолчанию пароль не задан. Данная строка остается пустой.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

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

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

5-5 ip http server

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

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

Параметры

Нет

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

В данном примере показан процесс включения сервера HTTP.

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

5-6 ip http secure-server

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

```
ip http secure-server
no ip http secure-server
```

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

В данном примере показан процесс включения HTTPS-сервера.

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

5-7 ip http access-class

Данная команда позволяет указать список, которому необходимо ограничить доступ к HTTP-серверу. При использовании формы **no** команда удалит список доступа из фильтра.

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

Параметры

<i>IP-ACL</i>	Стандартный список доступа IP-адресов. Поле адреса источника определяет доверенный или недоверенный узел.
---------------	---

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

В данном примере показан процесс создания стандартного списка доступа и назначение его для доступа к HTTP-серверу. Доступ к серверу дается только узлу 226.1.1.1.

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

5-8 ip http service-port

Данная команда позволяет указать порт HTTP. При использовании формы **no** команда вернется к настройкам по умолчанию.

```
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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет указать TCP-порт для сервера HTTP.

Пример

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

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

5-9 ip http timeout-policy idle

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

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

Параметры

<i>INT</i>	Значение таймера в секундах. Допустимый диапазон: от 60 до 36000
------------	--

По умолчанию

По умолчанию значение составляет 180 секунд.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

5-10 ip telnet server

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

```
ip telnet server
no ip telnet server
```

Параметры

Нет

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

В данном примере показан процесс включения сервера Telnet.

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

5-11 ip telnet service port

Данная команда позволяет задать порт 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

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

5-12 ip telnet source-interface

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

```
ip telnet source-interface INTERFACE-ID
no ip telnet source-interface
```

Параметры

<i>INTERFACE-ID</i>	IP-адрес интерфейса, который будет использоваться в качестве адреса источника пакетов при установке Telnet-соединения.
---------------------	--

По умолчанию

По умолчанию используется IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

5-13 line

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

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

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

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет войти в режим Line Configuration Mode.

Пример

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

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

5-14 service password-recovery

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

service password-recovery
no service password-recovery

Параметры

Нет

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

В данном примере показан процесс отключения функции восстановления пароля.

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

5-15 service password-encryption

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

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

Параметры

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

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

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

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

Пример

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

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

5-16 show terminal

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

show terminal

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

В данном примере показан процесс отображения информации о настройках терминала для текущей сессии.

```
Switch# show terminal

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

Switch#
```

5-17 show ip http server

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

show ip http server

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

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

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

5-18 show ip http secure-server

Данная команда используется для отображения информации о состоянии SSL.

show ip http secure-server

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения информации о состоянии SSL.

Пример

В данном примере показан процесс отображения информации о состоянии SSL.

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

5-19 show users

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

show users

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

В данном примере показан процесс отображения информации обо всех сессиях.

```
Switch# show users

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

Total Entries: 3

Switch#
```

5-20 telnet

Данная команда позволяет подключиться к другому устройству с поддержкой Telnet.

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

Параметры

<i>IP-ADDRESS</i>	IPv4-адрес узла.
<i>IPV6-ADDRESS</i>	IPv6-адрес узла.
<i>TCP-PORT</i>	Номер порта TCP. Диапазон портов TCP: от 1 до 65535. Как правило, для Telnet назначается TCP-порт 23.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная функция Telnet-клиента может быть использована для связи с другим устройством с помощью Telnet. ПО Telnet поддерживает особые команды в виде Telnet-последовательностей, которые преобразуют стандартные функции управления терминалом в функции, специфические для системы. Для выполнения Telnet-команды введите последовательность escape, а затем символ команды. Последовательность escape по умолчанию: CTRL+_ (нажмите и удерживайте CTRL, Shift и нижнее подчеркивание). Специфические команды Telnet будут отображаться следующим образом:

e - отключение от Telnet. Для отключения сессии Telnet может использоваться как прописная, так и строчная буква «e».

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

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

Пример

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

```
Switch# telnet 10.90.90.91

DGS-3130-30TS Gigabit Ethernet Switch

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

Password required, but none set

Switch#
```

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

```
Switch#telnet 10.90.90.91

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

Switch# telnet 10.90.90.91 3500

DGS-3130-30TS Gigabit Ethernet Switch

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

Password required, but none set

Switch#
```

5-21 terminal length

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

Уровень команды по умолчанию

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

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

Использование команды

При значении 0 отображение не прекратится, пока не будет достигнут конец 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#
```

5-22 terminal speed

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

terminal speed BPS
no terminal speed

Параметры

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

По умолчанию

Значение по умолчанию – 115200.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

5-23 session-timeout

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

session-timeout *MINUTES*
no session-timeout

Параметры

<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

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

5-24 terminal width

Данная команда используется для настройки количества столбцов символов, отображаемых на экране для текущей сессии. Команда **terminal width** влияет только на текущую сессию. Команда **terminal width default** установит значение по умолчанию, но не повлияет на текущую сессию.

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

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

Параметры

<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**

Уровень команды по умолчанию

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

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

Использование команды

По умолчанию ширина терминала составляет 80 символов. Команда **terminal width** позволяет изменить ширину терминала и применяется только к текущей сессии. При использовании формы **покоманда** вернет значение по умолчанию, то есть 80 символов.

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

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

Пример

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

```
Switch# show terminal

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

Switch# terminal width 120
Switch# show terminal

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

Switch #
```

5-25 username

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

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

Параметры

NAME	Имя пользователя, максимум 32 символа.
privilege LEVEL	(Опционально) Уровень привилегии для каждого пользователя. Диапазон доступных уровней: от 1 до 15.
nopassword	(Опционально) Указывает, что к данной учетной записи не будет применяться пароль.
password	(Опционально) Указывает, что к данной учетной записи будет применяться пароль.
0	(Опционально) Пароль в обычном текстовом виде. Длина пароля может составлять от 1 до 32 символов и содержать пробелы. Пароль чувствителен к регистру. Если синтаксис пароля не может быть указан, им будет обычный текст.
7	(Опционально) Пароль, зашифрованный на основе SHA-1. Длина пароля ограничена 35 байтами. Пароль чувствителен к регистру. Пароль зашифрован. Если синтаксис пароля не указан, им будет обычный текст.
15	(Опционально) Пароль, зашифрованный на основе MD5.

	Длина пароля ограничена 31 байтом. Пароль чувствителен к регистру. Пароль зашифрован. Если синтаксис пароля не указан, им будет обычный текст.
<i>PASSWORD</i>	(Опционально) Пароль на основе одного из указанных выше параметров.

По умолчанию

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

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

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

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

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

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

Пример

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

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

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

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

5-26 password

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

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

Параметры

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

По умолчанию

Нет

Режим ввода команды

Line Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

В данном примере показан процесс создания пароля для сессии консоли.

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

5-27 clear line

Данная команда используется для завершения сессии подключения.

```
clear line LINE-ID
```

Параметры

<i>LINE-ID</i>	Line ID сессии соединения, который необходимо отключить.
----------------	--

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Данная команда может отключить только сессии SSH и Telnet.

Пример

В данном примере показан процесс отключения сессии 1.

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

6. Команды предотвращения атак ARP Spoofing

6-1 ip arp spoofing-prevention

Команда используется для настройки записи ARP Spoofing Prevention (ASP), используемой для предотвращения атак ARP. 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.
<i>INTERFACE-ID</i>	Интерфейс, который будет активирован или удален из числа активных интерфейсов (при использовании формы no). Запись ARP не будет проверяться, если принимающий порт не включен в указанный список интерфейсов.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию записей нет.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

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

Указать можно только физические порты.

Пример

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

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

6-2 show ip arp spoofing-prevention

Данная команда используется для отображения настроек ARP Spoofing Prevention.

show ip arp spoofing-prevention

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения всех записей ARP Spoofing Prevention.

Пример

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

```
Switch# show ip arp spoofing-prevention

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

Total Entries: 1

Switch#
```

Отображаемые параметры

IP	IP-адрес шлюза.
----	-----------------

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

7. Команды Asymmetric VLAN

7-1 asymmetric-vlan

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

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

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для запуска/отключения функции Asymmetric VLAN.

Пример

В данном примере показано, как запустить функцию Asymmetric VLAN.

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

8. Команды Authentication, Authorization и Accounting (AAA)

8-1 aaa accounting commands

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

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

Параметры

<i>LEVEL</i>	Указывает выполнять учет для всех команд configure на указанном уровне прав доступа. Допустимые уровни привилегий прав доступа: от 1 до 15.
default	Указывает на настройку списка методов аккаунтинга по умолчанию.
<i>LIST-NAME</i>	Имя списка методов. Длина имени не должна превышать 32 символов.
<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>group tacacs+ – указывает на использование серверов, определенных командой TACACS+ server host.</p> <p>group GROUP-NAME – указывает на использование групп серверов, определенных командой aaa group server tacacs+.</p> <p>none – не выполнять аккаунтинг.</p>

По умолчанию

Метод аккаунтинга AAA не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для настройки списка методов аккаунтинга.

Пример

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

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

8-2 aaa accounting exec

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

```
aaa accounting exec {default | LIST-NAME} start-stop METHOD1 [METHOD2...]
no aaa accounting exec {default | LIST-NAME}
```

Параметры

default	Указывает на настройку списка методов аккаунтинга по умолчанию для EXEC.
<i>LIST-NAME</i>	Имя списка методов. Длина имени не должна превышать 32 символов.
<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>group radius – указывает на использование серверов, определенных командой RADIUS server host.</p> <p>group tacacs+ – указывает на использование серверов, определенных командой TACACS+ server host.</p> <p>group GROUP-NAME – указывает на использование групп серверов, определенных командой AAA group server.</p> <p>none – не выполнять аккаунтинг.</p>

По умолчанию

Метод аккаунтинга AAA не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для настройки списка методов аккаунтинга EXEC.

Пример

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

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

8-3 aaa accounting network

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

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

Параметры

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

По умолчанию

Метод аккаунтинга AAA не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

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

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

8-4 aaa accounting system

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

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

Параметры

system	Указывает на выполнение аккаунтинга событий системного уровня.
default	Указывает на настройку списка методов по умолчанию для аккаунтинга системных ресурсов.
start-stop	Указывает на отправку accounting-сообщений как в начальное, так и в конечное время доступа. Пользователям разрешен доступ к сети независимо от того, успешно ли будет включено начальное accounting-сообщение аккаунтинга
METHOD1 [METHOD2...]	<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>group radius – указывает на использование серверов, определенных командой RADIUS server host.</p> <p>group tacacs+ – указывает на использование серверов, определенных командой TACACS+ server host.</p> <p>group GROUP-NAME – указывает на использование групп серверов, определенных командой AAA group server.</p> <p>none – не выполнять аккаунтинг.</p>

По умолчанию

Метод аккаунтинга AAA не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

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

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

8-5 aaa authentication enable

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

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

Параметры

<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>enable – указывает на использование локального пароля для аутентификации.</p> <p>group radius – указывает на использование серверов, определенных командой RADIUS server host.</p> <p>group tacacs+ – указывает на использование серверов, определенных командой TACACS+ server host.</p> <p>group GROUP-NAME – указывает на использование групп серверов, определенных командой AAA group server.</p> <p>none – 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

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

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

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

8-6 aaa authentication dot1x

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

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

Параметры

METHOD1 [METHOD2...]

Укажите список методов, которые необходимо выполнить алгоритму аккаунтинга в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для указания метода.

local – указывает на использование локальной базы данных для аутентификации.

group radius – указывает на использование серверов, определенных командой RADIUS server host.

group GROUP-NAME – указывает на использование групп серверов, определенных командой AAA group server.

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

По умолчанию

Метод аутентификации AAA не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

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

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

8-7 aaa authentication igmp-auth

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

```
aaa authentication igmp-auth default group
radiusno aaa authentication igmp-auth default
```

Параметры

Нет

По умолчанию

Метод аутентификации AAA не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для настройки списка методов аутентификации по умолчанию для аутентификации IGMP.

Пример

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

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

8-8 aaa authentication login

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

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

Параметры

default	Указывает на настройку списка методов по умолчанию для аутентификации с именем пользователя.
<i>LIST-NAME</i>	Имя списка методов, отличного от списка методов по умолчанию. Длина имени не должна превышать 32 символов.
<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>local – указывает на использование локальной базы данных для аутентификации.</p> <p>group radius – указывает на использование серверов, определенных командой RADIUS server host.</p> <p>group tacacs+ – указывает на использование серверов, определенных командой TACACS+ server host.</p> <p>group GROUP-NAME – указывает на использование групп серверов, определенных командой AAA group server.</p> <p>none – 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

Уровень команды по умолчанию

Уровень 15

Использование команды

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

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

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

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

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

Пример

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

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

8-9 aaa authentication mac-auth

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

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

Параметры

<i>METHOD1 [METHOD2...]</i>	Укажите список методов, которые необходимо выполнить алгоритму аккаунтинга в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для указания метода.
-----------------------------	--

local – указывает на использование локальной базы данных для аутентификации.

group radius – указывает на использование серверов, определенных командой RADIUS server host.

group GROUP-NAME – указывает на использование групп серверов, определенных командой AAA group server.

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

По умолчанию

Метод аутентификации AAA не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

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

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

8-10 aaa authentication web-auth

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

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

Параметры

<i>METHOD1 [METHOD2...]</i>	Укажите список методов, которые необходимо выполнить алгоритму аккаунтинга в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для указания метода.
-----------------------------	--

local – указывает на использование локальной базы данных для аутентификации.

group radius – указывает на использование серверов, определенных командой RADIUS server host.

group GROUP-NAME – указывает на использование групп серверов, определенных командой AAA group server.

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

По умолчанию

Метод аутентификации AAA не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

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

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

8-11 aaa group server radius

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

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

Параметры

<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

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

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

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

8-12 aaa group server tacacs+

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

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

Параметры

<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

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

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

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

8-13 aaa new-model

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

```
aaa new-model
no aaa new-model
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

В данном примере показано, как включить функцию AAA.

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

8-14 accounting commands

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

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

Параметры

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

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Line Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

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

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


8-15 accounting exec

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

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

Параметры

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

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Line Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

В данном примере показано, как настроить список методов аккаунтинга EXEC с именем "list-1". Он использует сервер RADIUS. Если сервер безопасности не отвечает, он не выполняет аккаунтинг. После настройки аккаунтинг EXEC применяется к консоли.

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

8-16 clear aaa counters servers

Данная команда используется для сброса счетчиков статистики серверов AAA.

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

Параметры

all	Указывает на удаление информации счетчиков сервера,
------------	---

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

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

В данном примере показано, как сбросить счетчики серверов AAA.

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

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

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

8-17 ip radius source-interface

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

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

Параметры

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

По умолчанию

Будет использоваться IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode
Server Group Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

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

Пример

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

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

8-18 ip tacacs source-interface

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

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

Параметры

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

По умолчанию

Будет использоваться IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode Server Group Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

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

Пример

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

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

8-19 ipv6 radius source-interface

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

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

Параметры

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

По умолчанию

Будет использоваться IPv6-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode Server Group Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

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

Пример

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

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

8-20 ipv6 tacacs source-interface

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

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

Параметры

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

По умолчанию

Будет использоваться IPv6-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode Server Group Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Данная команда может применяться для указания интерфейса, чей IPv6-адрес будет использоваться в качестве IPv6-адреса источника для отправки пакетов TACACS. Если интерфейс источника указан как в режиме глобальной настройки, так и в режиме настройки группы серверов, то интерфейс источника, указанный в режиме настройки группы серверов, обладает приоритетом.

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

Пример

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

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

8-21 login authentication

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

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

Параметры

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

По умолчанию

По умолчанию используется список методов по умолчанию.

Режим ввода команды

Line Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

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

Пример

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

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

8-22 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

Уровень команды по умолчанию

Уровень 15

Использование команды

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

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

Пример

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

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

8-23 radius-server host

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

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

Параметры

<i>IP-ADDRESS</i>	IP-адрес сервера RADIUS.
<i>IPV6-ADDRESS</i>	IPv6-адрес сервера RADIUS.
auth-port <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.
acct-port <i>PORT-NUMBER</i>	(Опционально) Номер UDP-порта назначения для отправки пакетов аккаунтинга. Диапазон: от 0 до 65535. Укажите ноль в качестве значения номера порта, если узел сервера не предназначен для аккаунтинга. Значение по умолчанию: 1813.
timeout <i>SECONDS</i>	Значение тайм-аута сервера. Диапазон: от 1 до 255 секунд. Если значение не указано, то значением по умолчанию является 5 секунд.
retransmit <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.
0	(Опционально) Пароль в форме обычного незашифрованного текста. Это является опцией по умолчанию.
7	(Опционально) Пароль в зашифрованной форме.
key <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

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

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

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

8-24 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

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

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

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

8-25 server (TACACS+)

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

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

Параметры

<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

TACACS+ Group Server Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

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

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

8-26 show aaa

Данная команда используется для отображения глобального состояния AAA.

show aaa

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте эту команду для отображения глобального состояния AAA.

Пример

В данном примере показано, как отобразить глобальное состояние AAA.

```
Switch# show aaa

AAA is enabled.

Switch#
```

8-27 tacacs-server host

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

```
tacacs-server host {IP-ADDRESS | IPV6-ADDRESS} [port PORT] [timeout SECONDS] key [0 | 7] KEY-STRING
no tacacs-server host {IP-ADDRESS | IPV6-ADDRESS}
```

Параметры

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

По умолчанию

По умолчанию узел сервера TACACS+ не настроен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

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

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

8-28 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

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

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

```
Switch#show radius statistics
RADIUS Server: 172.19.192.80: Auth-Port 1645, Acct-Port 1646
State is UP

Auth.    Acct.
Round Trip Time:    10    10
Access Requests:    4     NA
Access Accepts:     0     NA
Access Rejects:     4     NA
Access Challenges:  0     NA
Acct Request:       NA     3
Acct Response:      NA     3
Retransmissions:    0     0
Malformed Responses: 0     0
Bad Authenticators: 0     0
Pending Requests:   0     0
Timeouts:           0     0
Unknown Types:      0     0
Packets Dropped:    0     0
```

Отображаемые параметры

Auth.	Статистика для пакетов аутентификации
Acct.	Статистика для пакетов аккаунтинга.
Round Trip Time	Интервал времени (в сотых долях секунды) между самым последним ответом и запросом, который соответствует ему, с этого сервера RADIUS.
Access Requests	Количество пакетов RADIUS Access-Request, отправленных на данный сервер. Не включает повторные передачи.
Access Accepts	Количество пакетов RADIUS Access-Асепт (действительных или недействительных), полученных с данного сервера.

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

8-29 show tacacs statistics

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

```
show tacacs statistics
```

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

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

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

Отображаемые параметры

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

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

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

9-2 arp timeout

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

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

Параметры

<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

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

9-3 clear arp-cache

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

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

Параметры

all	Укажите, чтобы полностью очистить кэш динамических ARP-записей, связанных со всеми интерфейсами.
<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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

9-4 ip address

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

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

Параметры

<i>IP-ADDRESS</i>	Укажите IP-адрес.
<i>SUBNET-MASK</i>	Укажите маску подсети для соответствующего IP-адреса.
secondary	(Опционально) Укажите, если настроенный адрес является вторичным IP-адресом. Если данное ключевое слово не указано, настроенный адрес будет являться первичным IP-адресом.
dhcp	Укажите, чтобы получить IP-адрес от DHCP-сервера.

По умолчанию

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

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

IPv4-адрес интерфейса может быть задан пользователем вручную или динамически (автоматически) назначен сервером DHCP. При настройке вручную пользователь может назначить в одну VLAN сразу

несколько сетей с IP-адресом для каждой. Один из этих IP-адресов должен быть основным IP-адресом, а остальные – второстепенными. Основной адрес используется в качестве IP-адреса источника для отправленных с интерфейса сообщений SNMP Trap или SYSLOG. Используйте команду **no ip address** для удаления заданного IP-адреса.

Пример

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

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

9-5 ip proxy-arp

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

ip proxy-arp
no ip proxy-arp

Параметры

Нет

По умолчанию

Данная опция по умолчанию отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

```
Switch# configure terminal
Switch(config)# interface vlan 100
Switch(config-if)# ip proxy-arp
Switch(config-if)#
```

9-6 ip local-proxy-arp

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

```
ip local-proxy-arp
no ip local-proxy-arp
```

Параметры

Нет

По умолчанию

Данная опция по умолчанию отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для включения опции local proxy ARP на интерфейсе. Команда используется в основной VLAN, относящейся к домену изолированной сети VLAN, для включения маршрутизации пакетов между второстепенными сетями VLAN или изолированными портами в пределах домена. Команда работает только после включения опции ip arp proxy.

Пример

В данном примере показано, как включить local proxy ARP на интерфейсе VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan 100
Switch(config-if)# ip local-proxy-arp
Switch(config-if)#
```

9-7 ip arp elevation

Данная команда используется для назначения более высокого приоритета всем ARP-пакетам этого коммутатора по сравнению с остальными ARP-пакетами.

```
ip arp elevation
no ip arp elevation
```

Параметры

Нет

По умолчанию

По умолчанию все ARP-пакеты имеют одинаковый приоритет.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для назначения всем ARP-пакетам этого коммутатора более высокого приоритета по сравнению с остальными ARP-пакетами.

Пример

В данном примере показано, как включить повышение приоритета IP ARP.

```
Switch# configure terminal
Switch(config)# ip arp elevation
Switch(config)#
```

9-8 ip mtu

Данная команда используется для настройки значения MTU. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ip mtu *BYTES*
no ip mtu

Параметры

<i>BYTES</i>	Укажите значение IP MTU. Диапазон допустимых значений: от 512 до 16383 байт.
--------------	--

По умолчанию

По умолчанию установлено значение MTU 1500 байт.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Некоторые протоколы маршрутизации, такие как OSPF, будут анонсировать этот параметр в обновлениях маршрутов.

Пример

В данном примере показано, как задать значение MTU размером 6000 байт для VLAN 4.

```
Switch# configure terminal
Switch(config)# interface vlan 4
Switch(config-if) ip mtu 6000
Switch(config-if)#
```

9-9 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. dynamic – для отображения только динамических ARP-записей. static – для отображения только статических ARP-записей.
ip-address [<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

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

В данном примере показано, как отобразить данные кэша ARP.

```
Switch# show arp
S - Static Entry
IP Address           Hardware Addr      IP Interface      Age (min)
-----
S 10.108.42.112      00-00-a7-10-4b-af  vlan 100          forever
10.108.42.114       00-00-a7-10-85-9b  vlan 200          forever
10.108.42.121       00-00-a7-10-68-cd  vlan 300          125

Total Entries: 3

Switch#
```

9-10 show arp timeout

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

show arp timeout [interface *INTERFACE-ID*]

Параметры

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

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

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

```
Switch# show arp timeout

Interface          Timeout (minutes)
-----
vlan 100           30
vlan 200           40

Total Entries: 2

Switch#
```

9-11 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.
brief	(Опционально) Укажите, чтобы отобразить информацию по IP-интерфейсу.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

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


```
Switch#show ip interface brief

Interface      IP Address      Link Status
-----
vlan 1         10.90.90.90     up
mgmt_ipif     192.168.0.1     down

Total Entries: 2

Switch#
```

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

```
Switch#show ip interface vlan 1

Interface vlan 1 is enabled, Link status is up
  IP address is 10.90.90.90/8 (Manual)
  ARP timeout is 240 minutes.
  IP MTU is 1500 bytes
  Helper Address is not set
  Proxy ARP is disabled
  IP Local Proxy ARP is disabled
  IP Directed Broadcast is disabled
  gratuitous-send is disabled, interval is 0 seconds

Total Entries: 1

Switch#
```

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

```
Switch#show ip interface loopback 1

Interface loopback1 is enabled
  IP address is 192.168.1.1/24 (Manual)

Total Entries: 1

Switch#
```

9-12 ip directed-broadcast

Данная команда используется для включения преобразования направленных широковещательных рассылок, получаемых интерфейсом, в рассылки канального уровня, когда сеть назначения подключена непосредственно к коммутатору. Используйте форму **no**, чтобы отключить преобразование.

```
ip directed-broadcast
no ip directed-broadcast
```

Параметры

Нет

По умолчанию

Данная опция по умолчанию отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для настройки на интерфейсе направленной широковещательной рассылки. Данная команда не влияет на маршрутизацию одноадресных пакетов, передачу пакетов направленной широковещательной рассылки за пределы локальной сети. Данная команда влияет только на передачу пакетов направленной широковещательной рассылки, для которых сети назначения являются локальными подсетями коммутатора. При включении опции направленной широковещательной рассылки пакеты будут преобразованы в широковещательные и направлены всем узлам сети назначения. В качестве интерфейса отправки может использоваться интерфейс получения или другие интерфейсы коммутатора.

Пример

В данном примере показано, как включить направленную широковещательную рассылку для интерфейса VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan 100
Switch(config-if)# ip directed-broadcast
Switch(config-if)#
```

10. Базовые команды настройки IPv6

10-1 clear ipv6 neighbors

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

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

Параметры

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

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

10-2 ipv6 address

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

```
ipv6 address {IPV6-ADDRESS/PREFIX-LENGTH / PREFIX-NAME SUB-BITS/PREFIX-LENGTH | IPV6-ADDRESS link-local}
no ipv6 address {IPV6-ADDRESS/PREFIX-LENGTH | PREFIX-NAME SUB-BITS/PREFIX-LENGTH | IPV6-ADDRESS link-local}
```

Параметры

<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес и длину префикса для подсети.
----------------------------	--

<i>PREFIX-LENGTH</i>	Укажите длину префикса. Префикс IPv6-адреса также является локальной подсетью на интерфейсе.
<i>PREFIX-NAME SUB-BITS</i>	Укажите имя префикса, используя не более 12 символов без пробелов.
<i>SUB-BITS</i>	Укажите сетевую и узловую части IPv6-адреса.
link-local	Укажите адрес Link-Local.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

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

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

Пример

В данном примере 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
```

В данном примере показано, как настроить IPv6-адрес на базе основного префикса, полученного клиентом DHCPv6. Глобальный адрес будет сконфигурирован после получения клиентом DHCPv6 основного префикса. Предположим, что общий префикс – 2001:2:3/48, а итоговый IPv6-адрес – 2001:2:3:4:5::3/64.

```
Switch# configure terminal
Switch(config)# interface vlan 2
Switch(config-if)# ipv6 address dhcp-prefix 1:2:3:4:5::3/64
```

В данном примере показано, как отменить формирование IPv6-адреса на основе префикса, полученного DHCPv6-клиентом.

```
Switch# configure terminal
Switch(config)# interface vlan 2
Switch(config-if)# no ipv6 address dhcp-prefix 0:0:0:2::3/64
```

10-3 ipv6 address eui-64

Данная команда используется для настройки на интерфейсе IPv6-адреса с использованием идентификатора интерфейса EUI-64 (Interface ID). Используйте форму **no**, чтобы удалить IPv6-адрес интерфейса с идентификатором EUI-64.

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

Параметры

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

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

В данном примере показано, как добавить IPv6-адрес.

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

10-4 ipv6 address dhcp

Данная команда используется для настройки интерфейса на получение IPv6-адреса с помощью DHCPv6. Используйте форму **no**, чтобы отключить использование DHCPv6 для получения IPv6-адреса.

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

Параметры

rapid-commit	Укажите, чтобы получать сетевые настройки от DHCP-сервера посредством быстрого обмена двумя сообщениями вместо стандартных четырех между Requesting Router (RR) и Delegating Router (DR).
---------------------	---

По умолчанию

Данная опция по умолчанию отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для настройки интерфейса на получение сетевых настроек IPv6 от сервера DHCPv6.

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

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

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

Пример

В данном примере показано, как настроить 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 address autoconfig

Данная команда используется для автоматической настройки IPv6-адреса с помощью механизма автоконфигурации Stateless autoconfiguration. Используйте форму **no**, чтобы удалить IPv6-адрес, сгенерированный с помощью механизма автоконфигурации.

```
ipv6 address autoconfig  
no ipv6 address autoconfig
```

Параметры

Нет

По умолчанию

Данная опция по умолчанию отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для IPv6-адреса интерфейса VLAN. Опция автоконфигурации по умолчанию отключена.

При включении автоконфигурации интерфейс включает обработку IPv6 и получает анонс от маршрутизатора IPv6 с назначенным префиксом глобального адреса. Далее итоговый адрес, состоящий из префикса и идентификатора интерфейса, назначается данному интерфейсу.

В случае отключения этой опции полученный Global Unicast-адрес будет удален из интерфейса.

Пример

В данном примере показано, как автоматически сконфигурировать IPv6-адрес, используя механизм Stateless auto-configuration.

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

10-6 ipv6 enable

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

```
ipv6 enable  
no ipv6 enable
```

Параметры

Нет

По умолчанию

Данная опция по умолчанию отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

10-7 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

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

По умолчанию

Значение по умолчанию – 64.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

В данном примере показано, как задать значение Hop Limit для IPv6.

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

10-8 ipv6 mtu

Данная команда используется для настройки значения MTU для IPv6. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ipv6 mtu BYTES
no ipv6 mtu
```

Параметры

<i>BYTES</i>	Укажите, чтобы задать значение MTU для IPv6. Допустимые значения - от 1280 до 65534 байт.
--------------	---

По умолчанию

По умолчанию для IPv6 установлено значение MTU 1500 байт.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурации интерфейса L3. Используйте эту команду для настройки значения MTU, которое будет анонсироваться в сообщениях RA. Пакет IPv6, сгенерированный в системе, будет передаваться на основе этого значения. Проверка выполняется на выходе. Пакеты свыше 1518 байт (oversize) будут отправлены вышестоящему blade-серверу для дальнейшей обработки.

Пример

В данном примере показано, как задать значение IPv6 MTU размером 6000 байт для VLAN 4.

```
Switch# configure terminal
Switch(config)# interface vlan 4
Switch(config-if) ipv6 mtu 6000
Switch(config-if)# exit
Switch(config)#
```

В данном примере показано, как восстановить значение MTU, заданное по умолчанию.

```
Switch# configure terminal
Switch(config)# interface vlan 4
Switch(config-if)# no ipv6 mtu
Switch(config-if)#
```

10-9 ipv6 nd managed-config-flag

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

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

Параметры

Нет

По умолчанию

Данный функционал по умолчанию отключен.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

10-10 ipv6 nd other-config-flag

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

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

Параметры

Нет

По умолчанию

Данный функционал по умолчанию отключен.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

В данном примере показано, как включить флаг O для получения других параметров конфигурации.

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

10-11 ipv6 nd prefix

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

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

Параметры

<i>IPV6-PREFIX/PREFIX-LENGTH</i>	Укажите IPv6-префикс, который будет сгенерирован или анонсирован в сообщении RA на интерфейсе.
<i>VALID-LIFETIME</i>	(Опционально) Укажите период времени в секундах, в

	течение которого префикс будет действителен. Допустимые значения: от 0 до 4294967295. Если значение не задано, устанавливается значение по умолчанию – 2592000 секунд (30 дней).
<i>PREFERRED-LIFETIME</i>	(Опционально) Укажите предпочтительное время жизни префикса в секундах. Допустимые значения: от 0 до 4294967295. Если значение не задано, устанавливается значение по умолчанию – 604800 секунд (7 дней).
off-link	(Опционально) Укажите, чтобы отключить флаг наличия соединения on-link. Если значение не задано, по умолчанию устанавливается флаг off-link.
no-autoconfig	(Опционально) Укажите, чтобы отключить флаг auto-configure. Если значение не задано, флаг auto-configure включается по умолчанию.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Статус префикса представлен следующими комбинациями:

- Комбинация 1: Опции off-link и no-autoconfig не заданы. Префикс добавляется в таблицу маршрутизации. Бит L = 1, бит A = 1.
- Комбинация 2: Задана опция no-autoconfig. Префикс добавляется в таблицу маршрутизации. Бит L = 1, бит A = 0.
- Комбинация 3: Задана опция off-link. Префикс не добавляется в таблицу маршрутизации. Бит L = 0, бит A = 1.

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

Пример

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

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

10-12 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Минимальный временной интервал не может быть меньше 3 секунд.

Пример

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

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

10-13 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

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

По умолчанию

Значение по умолчанию – 1800 секунд.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

В данном примере показано, как задать время жизни в анонсируемых сообщениях RA.

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

10-14 ipv6 nd suppress-ra

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

```
ipv6 nd suppress-ra
no ipv6 nd suppress-ra
```

Параметры

Нет

По умолчанию

Анонсирование RA на интерфейсе VLAN отключено.
Анонсирование RA на интерфейсе туннеля отключено.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду **ipv6 nd suppress-ra**, чтобы отключить отправку сообщений RA на интерфейсе. Используйте команду **no ipv6 nd suppress-ra**, чтобы включить отправку сообщений RA на интерфейсе туннеля ISATAP.

Пример

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

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

10-15 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>	Укажите время доступности для отправляемых анонсов маршрутизатора(в миллисекундах). Допустимые значения: от 0 до 3600000, кратно 1000.
----------------------	--

По умолчанию

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

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

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

Пример

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

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

10-16 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

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

В данном примере показано, как настроить отставку 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)#
```

10-17 ipv6 neighbor

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

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

Параметры

<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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для создания статической записи в таблице IPv6 neighbor cache на интерфейсе. Отслеживание достижимости соседних узлов к статическим записям не применяется.

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

Пример

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

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

10-18 show ipv6 general-prefix

Данная команда используется для просмотра информации по основному IPv6-префиксу.

```
show ipv6 general-prefix [PREFIX-NAME]
```

Параметры

<i>PREFIX-NAME</i>	(Опционально) Укажите имя основного префикса, для которого необходимо отобразить информацию. Если имя основного префикса не указано, будет отображаться информация по всем основным префиксам. Имя префикса
--------------------	---

не должно превышать 12 символов.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду для просмотра информации по основным IPv6-префиксам.

Пример

В данном примере показано, как отобразить информацию по всем основным IPv6-префиксам.

```
Switch# show ipv6 general-prefix

IPv6 prefix yy
Acquired via DHCPv6 PD
  vlan 1: 200::/48
    Valid lifetime 2592000, preferred lifetime 604800
Apply to interfaces
  vlan 2: ::2/64

Total Entries: 1

Switch#
```

10-19 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.
brief	(Опционально) Укажите, чтобы получить краткую информацию.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду для просмотра настроек конфигурации IPv6-интерфейса. Для интерфейса IPv6-туннеля будет отображаться только туннель ISATAP.

Пример

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

```
Switch# show ipv6 interface vlan 2

vlan 2 is up, Link status is down
IPv6 is enabled,
link-local address:
    FE80::201:1FF:FE02:305
Global unicast address:
    200::2/64 (DHCPv6 PD)
IPv6 MTU is 1500 bytes
RA messages are sent between 66 to 200 seconds
RA advertised reachable time is 1200000 milliseconds
RA advertised retransmit interval is 0 milliseconds
RA advertised life time is 1800 seconds
RA advertised O flag is OFF, M flag is OFF
RA advertised prefixes
200::/64
valid lifetime is 2592000, preferred lifetime is 604800

Switch#
```

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

```
Switch# show ipv6 interface brief

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

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

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

Total Entries: 3

Switch#
```

10-20 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

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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

Пример

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

```
Switch# show ipv6 neighbors

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

Total Entries: 1

Switch#
```

Отображаемые параметры

Тип записи	D – динамическая изученная запись. S – статическая neighbor-запись.
Состояние записи	INCMР (неполное) – состояние, когда запрос на получение адреса для записи отправлен, но ответное сообщение Neighbor Advertisement еще не получено. REACH (достижимое) – состояние, когда сообщение Neighbor Advertisement уже получено, а время таймера Reachable Time (в миллисекундах) еще не истекло. Это означает, что соседнее устройство работает корректно. STALE – состояние, в которое переходит запись, если с момента получения последнего подтверждения прошло

больше заданного таймером Reachable Time времени (в миллисекундах).

PROBE – состояние записи, при котором устройство отправляет сообщение Neighbor Solicitation, чтобы подтвердить достижимость.

11. Команды BPDU Protection

11-1 spanning-tree bpd protection (global)

Данная команда используется для общего включения функции BPDU Protection. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
spanning-tree bpd protection
no spanning-tree bpd protection
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Для экономии ресурсов системы можно предотвратить получение пакетов STP BPDU некоторыми из портов устройства.

Функция BPDU Protection предотвращает получение пакетов BPDU на указанных портах. При обнаружении коммутатором BPDU-атак есть три варианта защиты порта:

- **Drop** – коммутатор отбрасывает только полученные пакеты STP BPDU, порт остается в рабочем состоянии.
- **Block** – коммутатор отбрасывает все полученные BPDU-пакеты и блокирует все данные, порт остается в рабочем состоянии.
- **Shutdown** – коммутатор отключает порт, после чего порт переходит в состояние Error-Disabled.

Пример

В данном примере показано общее включение функции BPDU Protection.

```
Switch# configure terminal
Switch(config)# spanning-tree bpd protection
Switch(config)#
```

11-2 spanning-tree bpd protection (Interface)

Данная команда используется для включения функции BPDU Protection на порту. Используйте форму **no**, чтобы отключить функцию BPDU Protection на порту.

spanning-tree bpd protection {drop | block | shutdown}
no spanning-tree bpd protection

Параметры

drop	Укажите, чтобы отбросить все принимаемые BPDU-пакеты при обнаружении атаки.
block	Укажите, чтобы отбросить все пакеты (включая BPDU и обычные пакеты) при обнаружении атаки.
shutdown	Укажите, чтобы отключить интерфейс при обнаружении атаки.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения и настройки режима работы BPDU Protection. Команда также используется для конфигурации интерфейса порта и port-channel.

Пример

В данном примере показано, как включить функцию BPDU Protection в режиме block на Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# spanning-tree bpd protection block
Switch(config-if)#
```

11-3 show spanning-tree bpd protection

Данная команда используется для отображения информации о BPDU Protection.

show spanning-tree bpd protection [interface INTERFACE-ID [, | -]]

Параметры

interface INTERFACE-ID	(Опционально) Укажите ID интерфейса.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов

	от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения информации о BPDU Protection. Если не указан ID ни одного из интерфейсов, будет отображена информация обо всех интерфейсах.

Пример

В данном примере отображена информация о BPDU Protection и статусах интерфейсов.

```
Switch#show spanning-tree bpd-protection

Global State:      Enabled

Interface          State      Mode      Status
-----
eth1/0/1           Enabled   Shutdown  Under Attack
eth1/0/2           Enabled   Drop      Normal
eth1/0/3           Disabled  Block     -
eth1/0/4           Disabled  Shutdown  Normal
eth1/0/5           Disabled  Shutdown  Normal
eth1/0/6           Disabled  Shutdown  Normal
eth1/0/7           Disabled  Shutdown  Normal
eth1/0/8           Disabled  Shutdown  Normal
eth1/0/9           Disabled  Shutdown  Normal
eth1/0/10          Disabled  Shutdown  Normal
eth1/0/11          Disabled  Shutdown  Normal
eth1/0/12          Disabled  Shutdown  Normal
eth1/0/13          Disabled  Shutdown  Normal
eth1/0/14          Disabled  Shutdown  Normal
eth1/0/15          Disabled  Shutdown  Normal
eth1/0/16          Disabled  Shutdown  Normal
eth1/0/17          Disabled  Shutdown  Normal
eth1/0/18          Disabled  Shutdown  Normal
eth1/0/19          Disabled  Shutdown  Normal
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

В данном примере отображена информация статуса BPDU Protection для Ethernet 1/0/1.


```
Switch#show spanning-tree bpdu-protection interface ethernet 1/0/1

Interface      State      Mode      Status
-----      -
eth1/0/1      Enabled   Shutdown  Under Attack

Switch#
```

Отображаемые параметры

Interface	На интерфейсе включена функция BPDU Protection.
State	Отображает состояние конфигурации интерфейса.
Mode	Отображает режим работы интерфейса.
Status	Указывает, находится ли интерфейс в состоянии защиты.

11-4 snmp-server enable traps stp-bpdu-protection

Данная команда используется для запуска отправки SNMP-уведомлений (notification) для BPDU Protection. Используйте форму **no**, чтобы отключить отправку SNMP-уведомлений (notification) для BPDU Protection.

```
snmp-server enable traps stp-bpdu-protection
no snmp-server enable traps stp-bpdu-protection
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Нет

Пример

В данном примере показано, как включить отправку SNMP-уведомлений (notification) для BPDU Protection.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps stp-bpdu-protection
Switch(config)#
```

12. Команды Cable Diagnostics

12-1 test cable-diagnostics

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

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

Параметры

interface <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

Уровень команды по умолчанию

Уровень 1

Использование команды

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

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

Пример

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

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

12-2 show cable-diagnostics

Данная команда используется для просмотра результатов диагностики кабеля.

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

Параметры

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

По умолчанию

Нет

Режим ввода команды

EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения результатов диагностики кабеля.

Пример

Просмотр результатов диагностики кабеля.

```
Switch#show cable-diagnostics
```

Port	Type	Link Status	Test Result	Cable Length (M)
eth1/0/1	1000BASE-T	Link Down	Shutdown	2
eth1/0/2	1000BASE-T	Link Down	-	-
eth1/0/3	1000BASE-T	Link Down	-	-
eth1/0/4	1000BASE-T	Link Down	-	-
eth1/0/5	1000BASE-T	Link Down	-	-
eth1/0/6	1000BASE-T	Link Down	-	-
eth1/0/7	1000BASE-T	Link Down	-	-
eth1/0/8	1000BASE-T	Link Down	-	-
eth1/0/9	1000BASE-T	Link Down	-	-
eth1/0/10	1000BASE-T	Link Down	-	-
eth1/0/11	1000BASE-T	Link Down	-	-
eth1/0/12	1000BASE-T	Link Down	-	-
eth1/0/13	1000BASE-T	Link Down	-	-
eth1/0/14	1000BASE-T	Link Down	-	-
eth1/0/15	1000BASE-T	Link Down	-	-
eth1/0/16	1000BASE-T	Link Down	-	-
eth1/0/17	1000BASE-T	Link Down	-	-
eth1/0/18	1000BASE-T	Link Down	-	-
eth1/0/19	1000BASE-T	Link Down	-	-
eth1/0/20	1000BASE-T	Link Down	-	-
eth1/0/21	1000BASE-T	Link Down	-	-
eth1/0/22	1000BASE-T	Link Down	-	-
eth1/0/23	1000BASE-T	Link Down	-	-
eth1/0/24	1000BASE-T	Link Down	-	-

```
Switch#
```

12-3 clear cable-diagnostics

Данная команда используется для очистки результатов диагностики кабеля.

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

Параметры

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

По умолчанию

Нет

Режим ввода команды

EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для очистки результатов диагностики кабеля. При проведении диагностики на интерфейсе будет отображена ошибка.

Пример

В данном примере показано, как очистить результаты диагностики кабеля.

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

13. Команды логирования выполненных команд

13-1 command logging enable

Данная команда используется для включения функции логирования выполненных команд. При использовании формы **no** команда отключит функцию логирования.

```
command logging enable
no command logging enable
```

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команды логирования используются для записи списка команд, успешно выполненных через интерфейс командной строки. В журнале ведется запись введенных команд и информации об учетной записи пользователя, в которой была введена команда. Команды, не изменяющие конфигурацию или работу коммутатора (например, **show**), не записываются. Информация о сохранении и просмотре системного журнала описана в характеристиках sys-log.



Примечание: если коммутатор находится в режиме BAT (процедура загрузки, загрузка конфигурационного файла и т.д.), никакая из команд конфигурации не логируется (не будет записана в журнал).

Пример

В данном примере показан процесс включения функции логирования.

```
Switch# configure terminal
Switch(config)# command logging enable
Switch(config)#
```

14. Команды Connectivity Fault Management (CFM)

14-1 cfm global enable

Данная команда используется для общего включения функции CFM. Используйте форму **no** для общего отключения данной функции.

```
cfm global enable
no cfm global enable
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для общего включения/выключения CFM.

Пример

Общее включение CFM.

```
Switch# configure terminal
Switch(config)# cfm global enable
Switch(config)#
```

14-2 cfm domain

Данная команда используется для определения MD (домена технического обслуживания). Используйте форму **no** для удаления MD.

```
cfm domain DOMAIN-NAME level LEVEL
no cfm domain DOMAIN-NAME
```

Параметры

<i>DOMAIN-NAME</i>	Укажите имя MD. Максимальная длина строки – 22 символа. Использование пробелов недопустимо.
--------------------	--

level LEVEL	Укажите уровень MD: от 0 до 7.
--------------------	--------------------------------

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для назначения MD или входа в режим конфигурации CFM MD. Для лучшей идентификации административной ответственности каждому MD присваивается уникальное имя, отличное от уже используемых или доступных провайдеру/оператору. Для определения иерархической структуры каждому MD присваивается уникальный уровень обслуживания (от 0 до 7). Чем больше диапазон MD, тем выше уровень обслуживания.

Если имя MD введено некорректно или такое имя уже существует, в регистрации нового MD будет отказано. При удалении MD удаляются все сопутствующие настройки.

Пример

В данном примере показано, как назначить MD под именем «op-domain». Указанный уровень MD – 2.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)#
```

14-3 cfm ma

Данная команда используется для назначения МА (ассоциации технического обслуживания), а также входа в режим CFM MA Configuration. Используйте форму **no** для удаления МА.

cfm ma name MA-NAME [vlan VLAN-ID]
no cfm ma name MA-NAME

Параметры

name MA-NAME	Укажите МА с именем в качестве идентификатора.
vlan VLAN-ID	(Опционально) Укажите ID первичной VLAN под управлением МА.

По умолчанию

Нет

Режим ввода команды

CFM MD Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для назначения/удаления МА, а также входа в режим конфигурации CFM МА. У каждой ассоциации технического обслуживания в MD должно быть уникальное имя. У МА, настроенных в разных MD, могут совпадать идентификаторы МА. При создании МА необходимо указать ID первичной VLAN или войти в режим CFM MD Configuration для уже созданных МА. При удалении МА удаляются все сопутствующие настройки.

Пример

В данном примере показано, как создать МА под именем «op1», закрепленную за op-доменом под именем MD.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# cfm ma name op1 vlan 2
Switch(config-cfm-ma)#
```

14-4 mip creation (cfm md configuration)

Данная команда используется для настройки правила создания MIP (Maintenance Intermediate Points – промежуточные точки обслуживания) в MD. Используйте форму по, чтобы вернуться к настройкам по умолчанию.

mip creation {none | auto | explicit}
no mip creation

Параметры

none	Укажите, чтобы отказаться от создания MIP для МА в данном MD.
auto	Укажите, чтобы создать MIP на порту для МА в данном MD, если: <ul style="list-style-type: none"> на порту отсутствуют MEP (Maintenance End Points – конечные точки обслуживания) для МА с таким же VID на данном уровне MD или активных уровнях MD выше; на порту настроены MEP для МА с таким же VID на следующем активном уровне MD ниже; отсутствует МА с таким же VID на активных уровнях MD ниже. <p>Укажите параметр auto, чтобы создать MIP на промежуточном коммутаторе в МА.</p>
explicit	Укажите, чтобы создать MIP на порту для МА в данном MD, если:

- на порту отсутствуют MEP для MA с таким же VID наданном уровне MD или активных уровнях MD выше;
- на порту настроены MEP для MA с таким же VID на следующем активном уровне MD ниже.

По умолчанию

Параметр по умолчанию – **none**.

Режим ввода команды

CFM MD Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки правила создания MIP для домена технического обслуживания.

MIP на MD помогают отслеживать ссылки, MIP by MIP, а также позволяют пользователю выполнять закольцовывание от MEP к MIP. Чтобы узнать, может ли управляющий объект создать MHF (MIP Half Functions) для домена технического обслуживания, обратитесь к перечню создания MIP.

Настройки данной команды являются настройками по умолчанию для MA в данном MD при создании MIP. Используйте команду **mip creation** в режиме CFM MA Configuration Mode, чтобы применить настройки по умолчанию.

Пример

В данном примере показано, как настроить правило создания MIP при помощи параметра «auto».

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# mip creation auto
Switch(config-cfm-md)#
```

14-5 mip creation (cfm ma configuration)

Данная команда используется для настройки правила создания MIP для MA. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
mip creation {none | auto | explicit | defer}
no mip creation
```

Параметры

none	Укажите, чтобы отказаться от создания MIP для MA в данном MD.
auto	Укажите, чтобы создать MIP на порту для MA в данном MD,если:

- на порту отсутствуют MEP (Maintenance End Points – конечные точки обслуживания) для МА с таким же VID на данном уровне MD или активных уровнях MD выше;
- на порту настроены MEP для МА с таким же VID на следующем активном уровне MD ниже;
- отсутствует МА с таким же VID на активных уровнях MD ниже.

Укажите параметр **auto**, чтобы создать MIP на промежуточном коммутаторе в МА.

explicit

Укажите, чтобы создать MIP на порту для МА в данном MD, если:

- на порту отсутствуют MEP для МА с таким же VID на данном уровне MD или активных уровнях MD выше;
- на порту настроены MEP для МА с таким же VID на следующем активном уровне MD ниже.

defer

Укажите, чтобы применить настройки создания MIP для MD, в котором находится МА.

По умолчанию

Параметр по умолчанию – **defer**.

Режим ввода команды

CFM MA Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки правила создания MIP для МА. По умолчанию правило подчиняется команде **mip creation** в режиме CFM MD Configuration.

MIP на МА помогают отслеживать ссылки, MIP by MIP, а также позволяют пользователю выполнять закольцовывание от MEP к MIP. Чтобы узнать, может ли управляющий объект создать MHF для МА, обратитесь к перечню создания MIP.

Пример

В данном примере показано, как создать ассоциацию технического обслуживания MIP при помощи параметра «auto».

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# cfm ma name op-mal vlan 2
Switch(config-cfm-ma)# mip creation auto
Switch(config-cfm-ma)#
```

14-6 sender-id (cfm md configuration)

Данная команда используется для настройки передачи ID TLV отправителя при помощи MP (Maintenance Points – точки обслуживания) в домене технического обслуживания. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

sender-id {none | chassis | manage | chassis-manage}
no sender-id

Параметры

none	Укажите, чтобы отказаться от передачи ID TLV отправителя.
chassis	Укажите для передачи ID TLV отправителя с информацией об ID шасси.
manage	Укажите для передачи ID TLV отправителя с информацией об управляемом адресе.
chassis-manage	Укажите для передачи ID TLV отправителя с информацией об ID шасси и управляемом адресе.

По умолчанию

ID отправителя по умолчанию – **none**.

Режим ввода команды

CFM MD Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки передачи ID TLV отправителя при помощи MP в MD. В перечне ID отправителя указано, что именно необходимо включить (если необходимо) в ID TLV отправителя, передаваемого при помощи MP, настроенных в данном MD.

Настройки данной команды являются настройками по умолчанию для передачи ID TLV отправителя MP для MA в данном MD. Используйте команду **sender-id** в режиме CFM MA Configuration Mode, чтобы применить настройки по умолчанию.

Пример

В данном примере показано, как настроить передачу ID TLV отправителя в режиме CFM MD Configuration Mode, чтобы MP передавали ID TLV отправителя с информацией об ID шасси.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# sender-id chassis
Switch(config-cfm-md)#
```

14-7 sender-id (cfm ma configuration)

Данная команда используется для настройки передачи ID TLV отправителя при помощи MP для MA. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**sender-id {none | chassis | manage | chassis-manage | defer}
no sender-id**

Параметры

none	Укажите, чтобы отказаться от передачи ID TLV отправителя. В режиме CFM hardware используется только этот параметр.
chassis	Укажите для передачи ID TLV отправителя с информацией об ID шасси.
manage	Укажите для передачи ID TLV отправителя с информацией об управляемом адресе.
chassis-manage	Укажите для передачи ID TLV отправителя с информацией об ID шасси и управляемом адресе.
defer	Укажите, чтобы применить настройки передачи ID отправителя для MD, в котором находится MA.

По умолчанию

Параметр по умолчанию – **defer**.

Режим ввода команды

CFM MA Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки передачи ID TLV отправителя при помощи MP для MA. В перечне ID отправителя указано, что именно необходимо включить (если необходимо) в ID TLV отправителя, передаваемого при помощи MP, настроенных в данной MA.

Пример

В данном примере показано, как настроить передачу ID TLV отправителя в режиме CFM MA Configuration Mode, чтобы MP передавали ID TLV отправителя с информацией об ID шасси.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# cfm ma name op-mal vlan 2
Switch(config-cfm-ma)# sender-id chassis
Switch(config-cfm-ma)#
```

14-8 mepid-list

Данная команда используется для создания/удаления перечня MEP ID.

mepid-list {add | delete} MEPID-LIST**Параметры**

add	Укажите, чтобы добавить MEP ID в перечень MEP ID указанных МА.
delete	Укажите, чтобы удалить MEP ID из перечня MEP ID указанных МА.
<i>MEPID-LIST</i>	Укажите MEP ID, который необходимо добавить/удалить из перечня MEP ID указанных МА. Допустимый диапазон: от 1 до 8191.

По умолчанию

Нет

Режим ввода команды

CFM MA Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для добавления MEP ID в перечень MEP ID / удаления MEP ID из перечня MEP ID указанной МА. Для добавления MEP ID в перечень используйте команду **mepid-list add**. Для удаления MEP ID из перечня используйте команду **mepid-list delete**. Перед тем, как указать MEP, его ID необходимо добавить в перечень MEP ID.

Пример

В данном примере показано, как добавить MEP ID 1 и MEP ID 2 в перечень MEP ID МА под именем op1.

```
Switch#configure terminal
Switch(config)#cfm domain op-domain level 2
Switch(config-cfm-md)#cfm ma name op1
Switch(config-cfm-ma)#mepid-list add 1,2
Switch(config-cfm-ma)#
```

14-9 mode

Данная команда используется для настройки режима CFM MA.

mode {software | hardware}**Параметры**

software	Указывает, что МА работает в режиме CFM Software.
hardware	Указывает, что МА работает в режиме CFM Hardware.

По умолчанию

Параметр по умолчанию – **software**.

Режим ввода команды

CFM MA Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Режим CFM Hardware предназначен для улучшения производительности ССМ (Continuity Check Message). В режиме CFM Hardware ССМ-пакет обрабатывается при помощи аппаратного оборудования, и использование CPU не является обязательным. В данном режиме также можно установить минимальное значение интервала ССМ – 3,3 мс, что невозможно в режиме CFM Software ввиду ограниченных возможностей CPU.

Режимы CFM Hardware и CFM Software можно использовать одновременно. Если применить режим CFM Hardware для МА, все МЕР в МА будут работать в данном режиме. При необходимости задать конкретные значения для ССМ в некоторых МА (например, интервал ССМ от 3,3 до 10 мс или наличие Down МЕР), пользователь может использовать режим CFM Hardware. Если значения процесса ССМ не критичны / необходимо установить Up МЕР или Up MIP / требуется наличие функции Full CFM, предпочтительнее выбрать режим CFM Software.

Пример

В данном примере показано, как настроить режим CFM МА.

```
Switch#configure terminal
Switch(config)#cfm domain op-domain level 2
Switch(config-cfm-md)#cfm ma name opl
Switch(config-cfm-ma)#mode hardware
Switch(config-cfm-ma)#
```

14-10 ccm interval

Данная команда используется для настройки интервала ССМ для МА. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ccm interval INTERVAL
no ccm interval
```

Параметры

<i>INTERVAL</i>	Укажите интервал ССМ:
3,3 мс:	3,3 миллисекунды. Применим только в режиме CFM Hardware.
10 мс:	10 миллисекунд. Применим только в режиме CFM Hardware.
100 мс:	100 миллисекунд. Не рекомендуется применять в режиме CFM Software, т. к. это может спровоцировать

загруженность CPU.

1 с: 1 секунда.

10 с: 10 секунд.

1 мин: 1 минута.

10 мин: 10 минут

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

CFM MA Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки интервала CCM для МА – периода времени, в течение которого MEP в МА отправляет CCM.

Пример

В данном примере показано, как настроить интервал CCM для МА.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# cfm ma name opl vlan 2
Switch(config-cfm-ma)# ccm interval 10sec
Switch(config-cfm-ma)#
```

14-11 cfm mep

Данная команда используется для назначения конечной точки ассоциации технического обслуживания и входа в режим CFM MEP Configuration Mode. Используйте форму **no**, чтобы удалить MEP.

cfm mep mepid *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* [**direction** {up | down}]
no cfm mep mepid *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME*

Параметры

mepid <i>MEP-ID</i>	Укажите MEP ID. Допустимый диапазон: от 1 до 8191.
name <i>MA-NAME</i>	Укажите имя МА.
direction	(Опционально) Укажите направление MEP.
up	Укажите, чтобы передавать PDU (CFM Protocol Data Units) по направлению к Bridge Relay Entity и получать их от направления Bridge Relay Entity, которое также называется Inward Facing (Up) MEP.
down	Укажите, чтобы передавать CFM PDU по направлению к LAN и получать их от направления LAN, которое также

называется Outward Facing MEP.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для назначения конечной точки ассоциации технического обслуживания. У MEP, настроенных в одной MA, должны быть уникальные MEP ID. У MEP в разных MA могут быть идентичные MEP ID. Перед тем, как создать MEP, их ID необходимо добавить в список MEP ID MA.

Пример

В данном примере показано, как настроить MEP на указанном физическом интерфейсе. Указанное направление MEP – Up.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# cfm mep mepid 1 ma name opl domain op-domain direction up
Switch(config-cfm-mep)#
```

14-12 cfm enable

Данная команда используется для запуска функции CFM на указанном физическом интерфейсе. Используйте форму **no**, чтобы отключить функцию CFM на указанном физическом интерфейсе.

cfm enable
no cfm enable

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения/выключения функции CFM на указанном физическом интерфейсе.

Пример

В данном примере показано, как включить функцию CFM на указанном физическом интерфейсе.

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

14-13 mep enable

Данная команда используется для запуска статуса MEP. Используйте форму **no**, чтобы отключить статус MEP.

mep enable
no mep enable

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

CFM MEP Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для запуска/отключения статуса MEP.

Пример

В данном примере показано, как запустить статус MEP.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#cfm mep mepid 1 ma name opl domain op-domain
Switch(config-cfm-mep)#mep enable
Switch(config-cfm-mep)#
```

14-14 pdu-priority

Данная команда используется для назначения приоритета 802.1p в CCM и других CFM PDU, передаваемых при помощи MEP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

pdu-priority *COS-VALUE*
no pdu-priority

Параметры

<i>COS-VALUE</i>	Установите приоритет 802.1p в CCM и других CFM PDU, передаваемых при помощи MEP. Допустимый диапазон: от 0 до 7.
------------------	--

По умолчанию

Приоритет PDU по умолчанию – 7.

Режим ввода команды

CFM MEP Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для назначения приоритета 802.1p в CCM и других CFM PDU, передаваемых при помощи MEP.

Пример

В данном примере показано, как назначить приоритет PDU MEP.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# cfm mep mepid 1 ma name opl domain op-domain
Switch(config-cfm-mep)# pdu-priority 2
Switch(config-cfm-mep)#
```

14-15 fault-alarm

Данная команда используется для получения оповещений о неисправностях и их типах при помощи MEP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

fault-alarm {*none* | *all* | *mac-status* | *remote-ccm* | *error-ccm* | *xcon-ccm*}
no fault-alarm

Параметры

none	Укажите, чтобы отказаться от получения оповещений о
-------------	---

	неисправностях.
all	Укажите, чтобы получать оповещения обо всех типах неисправностей.
mac-status	Укажите, чтобы получать оповещения о неисправностях, чей приоритет выше или равен DefMAC status.
remote-ccm	Укажите, чтобы получать оповещения о неисправностях, чей приоритет выше или равен DefRemoteCCM.
error-ccm	Укажите, чтобы получать оповещения о неисправностях, чей приоритет выше или равен DefErrorCCM.
xcon-ccm	Укажите, чтобы получать оповещения только о неисправностях DefXconCCM.

По умолчанию

Параметр по умолчанию – none.

Режим ввода команды

CFM MEP Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для указания типов неисправностей, о наличии которых вы будете получать уведомления при помощи MEP. Для мониторинга доступны следующие типы неисправностей: DefRDICCM, DefMAC status, DefRemoteCCM, DefErrorCCM и DefXconCCM. Приоритетность возрастает от первого указанного типа к последнему.

- **DefRDICCM:** последний CCM, полученный при помощи данных MEP от удаленных MEP, содержит бит RDI.
- **DefMACstatus:** согласно последнему CCM, полученному при помощи данных MEP от удаленных MEP, передача MAC, связанного с MEP, сообщает о состоянии ошибки при помощи Port Status TLV или Interface Status TLV.
- **DefRemoteCCM:** данные MEP не получают CCM от других MEP, указанных в списке конфигурации.
- **DefErrorCCM:** данные MEP получают неверные CCM.
- **DefXconCCM:** CCM, которые получают данные MEP, предположительно принадлежат другим MA.

Пример

В данном примере показано, как настроить MEP для отправки оповещений обо всех типах неисправностей.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# cfm mep mepid 1 ma name opl domain op-domain
Switch(config-cfm-mep)# fault-alarm all
Switch(config-cfm-mep)#
```

14-16 alarm-time

Данная команда используется для установки интервала отправки оповещений о неисправностях и сброса системы оповещений. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

alarm-time {delay CENTISECOND | reset CENTISECOND}
no alarm-time {delay | reset}

Параметры

delay CENTISECOND	Укажите интервал между обнаружением неисправности на MEP и отправкой оповещения. Единица измерения – сантисекунда. Допустимый диапазон: от 250 до 1000.
reset CENTISECOND	Укажите интервал между устранением неисправностей, обнаруженных на MEP, и сбросом оповещений. Единица измерения – сантисекунда. Допустимый диапазон: от 250 до 1000.

По умолчанию

Интервал для отправки оповещений MEP по умолчанию – 250.
 Интервал для сброса оповещений MEP по умолчанию – 1000.

Режим ввода команды

CFM MEP Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для установки интервала отправки оповещений о неисправностях с момента их обнаружения: соответствующее оповещение будет отправлено, если по истечении заданного периода времени неисправность не устранена.

После устранения всех неисправностей, обнаруженных на MEP, запускается таймер обратного отсчета. Если по истечении заданного периода неисправностей не обнаружено, будет выполнен сброс системы оповещений.

Пример

В данном примере показано, как настроить интервал отправки оповещений MEP. Заданное значение – 250 сантисекунд.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# cfm mep mepid 1 ma name opl domain op-domain
Switch(config-cfm-mep)# alarm-time delay 250
Switch(config-cfm-mep)#
```

В данном примере показано, как настроить интервал сброса оповещений MEP. Заданное значение – 1000 сантисекунд.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)# alarm-time reset 1000
Switch(config-cfm-mep)#
```

14-17 ccm enable

Данная команда используется для включения функции CCM (CFM Continuity Check Message). Используйте форму **no**, чтобы отключить данную функцию.

ccm enable
no ccm enable

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

CFM MEP Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения/выключения функции CFM CCM MEP.

Пример

В данном примере показано, как включить функцию CFM CCM MEP.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)# ccm enable
Switch(config-cfm-mep)#
```

14-18 show cfm counter ccm

Данная команда используется для отображения счетчиков CFM CCM всех MEP.

show cfm counter ccm

Параметры

Нет

По умолчанию

Нет

Режим ввода командыUser/Privileged EXEC Mode
Любой режим конфигурации**Уровень команды по умолчанию**

Уровень 1

Использование команды

Данная команда используется для отображения счетчиков пакета CCM RX всех MEP.

Пример

В данном примере показано, как отобразить счетчики пакета CCM всех MEP.

```
Switch#show cfm counter ccm

CCM counters:

MEPID: 1   VID: 2   Level: 2   Direction: Up   Port: 1/0/1
XCON: 9           Error: 8       Normal: 100
MEPID: 2   VID: 1   Level: 2   Direction: up   Port: 1/0/11
XCON: 9           Error: 8       Normal: 100

Total:
XCON: 18           Error: 16       Normal: 200

Switch#
```

Отображаемые параметры

XCON	Укажите для отображения количества полученных CCM с кросс-соединением.
Error	Укажите для отображения количества полученных CCM, которые являются недействительными.
Normal	Укажите для отображения количества полученных CCM, которые являются нормальными.

14-19 clear cfm counter ccm

Данная команда используется для обнуления счетчиков CCM всех MEP.

clear cfm counter ccm**Параметры**

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для обнуления счетчиков пакета CCM MEP.

Пример

В данном примере показано, как обнулить счетчики пакета CCM всех MEP.

```
Switch# clear cfm counter ccm
Switch#
```

14-20 cfm loopback test

Данная команда используется для запуска теста Loopback CFM.

cfm loopback test {*MAC-ADDR* | **remote-mepid** *REMOTE-MEPID*} **mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* [**num** *NUMBER*] [**length** *LENGTH*] **pattern** *STRING*] [**pdu-priority** *COS-VALUE*]

Параметры

<i>MAC-ADDR</i>	Укажите MAC-адрес получателя.
remote-mepid <i>REMOTE-MEPID</i>	Укажите MEP ID получателя.
mepid <i>MEP-ID</i>	Укажите MEP ID, на котором необходимо запустить функцию Loopback.
name <i>MA-NAME</i>	Укажите имя MA.
domain <i>DOMAIN-NAME</i>	Укажите имя MD. Максимальная длина строки – 22 символа.
num <i>NUMBER</i>	(Опционально) Укажите количество LBM для отправки. Значение по умолчанию – 4.
length <i>LENGTH</i>	(Опционально) Укажите длину полезной нагрузки LBM для отправки. Допустимый диапазон: от 0 до 1500. Значение по умолчанию – 0.
pattern <i>STRING</i>	(Опционально) Укажите, нужно ли использовать Data TLV. Если использование Data TLV необходимо, задайте нужное значение. Максимальная длина строки – 1500 символов. Использование пробелов

	недопустимо.
pdu-priority <i>COS-VALUE</i>	(Опционально) Установите приоритет 802.1p в передаваемых LBM. Если значение не задано, используется приоритет, идентичный приоритету CCM, отправляемым при помощи MEP.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте сочетание клавиш CTRL+C, чтобы завершить тест Loopback. В MAC-адресе отображаются MEP или MIP получателя, доступные данному MAC-адресу. Адрес может быть индивидуальным или групповым. На групповых адресах поддерживается функция Multicast Loopback. В MEP ID отображаются исходные MEP, используемые для запуска сообщения Loopback.

Пример

В данном примере показан процесс передачи LBM на MAC-адрес получателя 00-01-02-03-04-05.

```
Switch# cfm loopback test 00-01-02-03-04-05 mepid 1 ma name op-mal domain op-domain1

Request timed out.
Request timed out.
Request timed out.
Request timed out.
CFM loopback statistics for 00-01-02-03-04-05:
Packets: Sent=4, Received=0, Lost=4(100% loss).

Switch# cfm loopback test remote-mepid 2 mepid 1 ma name op-mal domain op-domain1

Reply from 00-01-02-03-04-05: bytes=0 time=10ms
Reply from 00-01-02-03-04-05: bytes=0 time=10ms
Reply from 00-01-02-03-04-05: bytes=0 time=10ms
Reply from 00-01-02-03-04-05: bytes=0 time=10ms
CFM loopback statistics for 00-01-02-03-04-05:
Packets: Sent=4, Received=4, Lost=0(0% loss).

Switch#
```

14-21 cfm linktrace

Данная команда используется для создания сообщения Link Trace.

cfm linktrace *MAC-ADDR* **mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* [**ttl** *TTL*][**pdu-priority** *COS-VALUE*]

Параметры

MAC-ADDR	Укажите MAC-адрес получателя.
mepid <i>MEP-ID</i>	Укажите MEP ID, на которых необходимо запустить функцию Link Trace.
name <i>MA-NAME</i>	Укажите имя MA.
domain <i>DOMAIN-NAME</i>	Укажите имя MD. Максимальная длина строки – 22 символа.
ttl <i>TTL</i>	(Опционально) Укажите значение TTL сообщения Link Trace. Допустимый диапазон: от 2 до 255. Значение по умолчанию – 64.
pdu-priority <i>COS-VALUE</i>	(Опционально) Установите приоритет 802.1p в передаваемых LTM. Если значение не задано, используется приоритет, идентичный приоритету CSM, отправляемым при помощи MEP.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для создания сообщения CFM Link Trace.

Пример

В данном примере показан процесс передачи LTM на MAC-адрес получателя 00-01-02-03-04-05.

```
Switch# cfm linktrace 00-01-02-03-04-05 mepid 1 ma name op-mal domain op-domain1
Transaction ID: 26
Switch#
```

14-22 show cfm linktrace

Данная команда используется для отображения ответов Link Trace.

show cfm linktrace [**mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* [**trans-id** *ID*]]

Параметры

mepid <i>MEP-ID</i>	(Опционально) Укажите MEP ID. Если значение не задано, будут отображены ответы Link Trace всех MEP.
name <i>MA-NAME</i>	(Опционально) Укажите имя MA.
domain <i>DOMAIN-NAME</i>	(Опционально) Укажите имя MD. Максимальная длина строки – 22 символа.
trans-id <i>ID</i>	(Опционально) Укажите для отображения идентификатора транзакции. Если значение не задано, будут отображены все транзакции MEP, на которых запущена функция Link Trace.

По умолчанию

Нет

Режим ввода командыUser/Privileged EXEC Mode
Любой режим конфигурации**Уровень команды по умолчанию**

Уровень 1

Использование команды

Данная команда используется для отображения ответов Link Trace. Максимально допустимое количество ответов Link Trace на устройство – 128.

Пример

В данном примере показано, как отобразить ответы Link Trace.

```
Switch# show cfm linktrace mepid 1 ma name op-ma domain op-domain trans-id 0

Transaction ID: 0
From MEPID 1 to 00-07-00-00-00-1C
Start Time: 2013-11-02 11:35:11
Hop: 1
  Ingress MAC Address: 00-00-00-00-00-00
  Egress MAC Address: 00-09-5A-B9-AC-1B
  Forwarded: Yes           Relay Action: FDB

Hop: 2
  MEPID: 2
  Ingress MAC Address: 00-07-00-00-00-1C
  Egress MAC Address: 00-00-00-00-00-00
  Forwarded: No           Relay Action: Hit

Switch#
```

Отображаемые параметры**Relay Action****Hit:** LTM достиг MP, MAC-адрес которых соответствует

целевому MAC-адресу.

FDB: выходной порт выбран в соответствии с информацией базы данных фильтрации.

MPDB: выходной порт выбран в соответствии с информацией баз данных MIP CCM.

14-23 clear cfm linktrace

Данная команда используется для удаления полученных ответов Link Trace.

```
clear cfm linktrace {mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME | all}
```

Параметры

mepid <i>MEP-ID</i>	Укажите MEP ID.
name <i>MA-NAME</i>	Укажите имя MA.
domain <i>DOMAIN-NAME</i>	Укажите имя MD. Максимальная длина строки – 22 символа.
all	Укажите, чтобы удалить всю информацию Link Trace для всех MEP.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для удаления из хранилища данных ответов Link Trace, запущенных при помощи указанных MEP.

Пример

В данном примере показано, как удалить полученные ответы Link Trace.

```
Switch# clear cfm linktrace mepid 1 ma name op-mal domain op-domain1
Switch#
```

14-24 ais

Данная команда используется для запуска и настройки параметров функции AIS (Alarm Indication Signal). Используйте форму **no**, чтобы отключить данную функцию.

```
ais [period PERIOD] [level LEVEL]
no ais [period | level]
```

Параметры

period <i>PERIOD</i>	(Опционально) Укажите интервал передачи AIS PDU: 1 секунда или 1 минута.
level <i>LEVEL</i>	(Опционально) Укажите уровень MD клиента, которому MEP посылают AIS PDU. Допустимый диапазон: от 0 до 7.

По умолчанию

По умолчанию данная функция отключена. Интервал по умолчанию – 1 секунда.

Режим ввода команды

CFM MEP Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для запуска на MEP функции AIS и настройки ее параметров. Если не указаны дополнительные параметры, функция AIS будет запущена автоматически. Если не указан уровень клиента, будет использован уровень MD, на котором существуют MIP и MEP слоя ближайшего клиента. Уровень домена технического обслуживания клиента по умолчанию может меняться в процессе создания или удаления домена технического обслуживания уровня выше или MA на устройстве.

При выявлении неисправности MEP могут начать циклическую передачу кадров, содержащих информацию об ETH-AIS на уровне клиента. MEP продолжают передачу кадров с информацией об ETH-AIS, пока не будет устранена неисправность. После получения кадра с информацией об ETH-AIS от слоя/sub-слоя соответствующего сервера, MEP слоя/sub-слоя клиента обнаружат статус AIS и отключат оповещения, связанные со всеми равными MEP. MEP возобновят отправку оповещений при обнаружении неисправностей, когда статус AIS будет отключен.

При отсутствии MIP и MEP слоя ближайшего клиента вычислить уровень MD клиента невозможно. Если уровень клиента не задан пользователем, а вычислить уровень MD клиента нельзя, передача AIS PDU невозможна.

Пример

В данном примере показан процесс настройки функции AIS, уровень клиента – 5.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# cfm mep mepid 1 ma name opl domain op-domain
Switch(config-cfm-mep)# ais level 5
Switch(config-cfm-mep)#
```

14-25 lck

Данная команда используется для включения функции LCK и настройки ее параметров. Используйте форму **no**, чтобы отключить данную функцию.

**lck [period PERIOD] [level LEVEL]
no lck [period | level]**

Параметры

period PERIOD	(Опционально) Укажите интервал передачи LCK PDU: 1 секунда или 1 минута. Интервал по умолчанию – 1 секунда.
level LEVEL	(Опционально) Укажите уровень MD клиента, которому MEP отсылает LCK PDU. Допустимый диапазон: от 0 до 7.

По умолчанию

По умолчанию данная функция отключена.
Интервал по умолчанию – 1 секунда.

Режим ввода команды

CFM MEP Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения на MEP функции LCK и настройки ее параметров. Если параметры не заданы, функция CFM LCK будет запущена автоматически. Если не указан уровень клиента, будет использован уровень MD, на котором существуют MIP и MEP слоя ближайшего клиента. Уровень домена технического обслуживания клиента по умолчанию может меняться в процессе создания или удаления домена технического обслуживания уровня выше, а также MA на устройстве.

При отсутствии MIP и MEP слоя ближайшего клиента вычислить уровень MD клиента по умолчанию невозможно. Если уровень клиента не задан пользователем, а вычислить уровень MD клиента по умолчанию нельзя, передача LCK PDU невозможна.

Пример

В данном примере показан процесс настройки функции LCK, уровень клиента – 5.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# cfm mep mepid 1 ma name opl domain op-domain
Switch(config-cfm-mep)# lck level 5
```

14-26 cfm lck start

Данная команда используется для включения блокировки от имени администратора. Используйте форму **no**, чтобы выключить блокировку.

cfm lck start mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME
cfm lck stop mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME

Параметры

mepid <i>MEP-ID</i>	Укажите MEP ID.
name <i>MA-NAME</i>	Укажите имя MA.
DOMAIN-NAME	Укажите имя MD. Максимальная длина строки – 22 символа.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения/выключения блокировки. При включении блокировки MEP отсылают LCK PDU на MEP уровня клиента. Проверить статус блокировки можно при помощи команды **show cfm mep**. Пункт LCK Action в команде **show cfm mep** отображает текущий статус блокировки – Start (запущен) или Stop (отключен).

Пример

В данном примере показано, как включить блокировку.

```
Switch# cfm lck start mepid 1 ma name op-ma domain op-domain
Switch#
```

14-27 snmp-server enable traps cfm

Данная команда используется для запуска статуса Trap ITU Y.1731 AIS и функции LCK. Используйте форму **no**, чтобы отключить AIS и статус LCK Trap.

```
snmp-server enable traps cfm [ais] [lck]
no snmp-server enable traps cfm [ais] [lck]
```

Параметры

ais	(Опционально) Укажите статус Trap AIS, который необходимо настроить. Если статус Trap AIS запущен, при появлении или удалении события ETH-AIS trap будет выслан.
lck	(Опционально) Укажите статус Trap LCK, который необходимо настроить. Если статус Trap LCK запущен, при появлении или удалении события ETH-LCK trap будет выслан.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для общей настройки статуса Trap функции ITU Y.1731. Если значение не задано, будут установлены статусы Trap AIS и LCK. Используйте команду **show cfm**, чтобы отобразить статус Trap ITU Y.1731.

Пример

В данном примере показан процесс запуска статуса Trap AIS.

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

14-28 lm enable

Данная команда используется для запуска функции LM (Loss Measurement) ITU Y.1731. Используйте форму **no**, чтобы отключить данную функцию.

lm enable
no lm enable

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

CFM MEP Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения/выключения функции LM. Когда функция Frame Loss Measurement запущена на MEP от имени администратора, MEP поддерживают счетчики функции Frame Loss Measurement и могут отвечать на сообщения LMR, получая сообщения LMM.

Пример

В данном примере показано, как запустить функцию LM.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#cfm mep mepid 1 ma name opl domain op-domain
Switch(config-cfm-mep)#lm enable
Switch(config-cfm-mep)#
```

14-29 cfm lm test

Данная команда используется для запуска теста LM на MEP.

cfm lm test *MAC-ADDR mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME* [period *PERIOD*] [pdu-priority *COS-VALUE*]

Параметры

mepid <i>MEP-ID</i>	Укажите MEP ID.
name <i>MA-NAME</i>	Укажите имя MA.
domain <i>DOMAIN-NAME</i>	Укажите имя MD. Максимальная длина строки – 22 символа.
period <i>PERIOD</i>	(Опционально) Укажите интервал передачи LM PDU: 100 мс, 1 с или 10 с. Интервал по умолчанию – 1 с.
pdu-priority <i>COS-VALUE</i>	(Опционально) Установите приоритет 802.1p в сообщениях LMM, передаваемых при помощи MEP. Значение по умолчанию – приоритет PDU MEP.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для запуска теста LM на MEP. MEP будут периодически отправлять сообщения LMM на удаленные MEP. Система рассчитает дальний и ближний FLR (Frame Loss Ratio – коэффициент потери кадров), основанный на полученных сообщениях LMR.

Пользователь может прервать тест Frame Loss Measurement, отключив функцию Frame Loss Measurement на MEP.

При использовании функции Frame Loss Measurement необходимо учитывать ограничения счетчиков.

- Подсчет невозможен в общем (MP-t-MP) Ethernet-соединении устройств, неизвестных одноадресных кадров, широковещательных и многоадресных кадров, передаваемых от удаленных MEP на Up MEP, или от Down MEP на удаленные MEP.
- Невозможно подсчитать PDU протокола, обрабатываемого при помощи ПО устройства.
- Использование функций ETH-LM/ETH-DM провоцирует расход ресурсов ACL устройства, что необходимо учитывать при запуске функций ETH-LM/ETH-DM, когда количество MEP слишком велико.

Пример

В данном примере показано, как запустить тест LM.

```
Switch# cfm lm test 00-01-02-03-04-05 mepid 1 ma name opl domain op-domain period 1sec pdu-
priority 7
Switch#
```

14-30 show cfm lm

Данная команда используется для отображения информации об LM.

show cfm lm [mepid *MEP-ID* ma name *MA-NAME* domain *DOMAIN-NAME*]

Параметры

mepid <i>MEP-ID</i>	Опционально) Укажите MEP ID.
name <i>MA-NAME</i>	(Опционально) Укажите имя MA.
domain <i>DOMAIN-NAME</i>	(Опционально) Укажите имя MD. Максимальная длина строки – 22 символа.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения информации об LM. Если не заданы опциональные параметры, будет отображена вся информация.

Пример

В данном примере показано, как отобразить информацию об LM.

```
Switch#show cfm lm mepid 1 ma name opl domain op-domain

MEP ID: 1
MA Name: opl
Domain Name: op-domain
State: Enabled
LMM Transmitted : 61
LMR Received   : 0
LMM Received   : 0
LMR Transmitted : 0

ID  MAC Address      Status  Period Pri Far-End Near-End Start Time
-----
1   00-01-02-03-04-05 Failed  1sec  2   0       0       2000-02-02 23:23:06

Switch#
```

14-31 clear cfm lm

Данная команда используется для удаления информации о функции LM.

```
clear cfm lm {mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME [result | statistics] | all}
```

Параметры

mepid <i>MEP-ID</i>	Укажите MEP ID.
name <i>MA-NAME</i>	Укажите имя MA.
domain <i>DOMAIN-NAME</i>	Укажите имя MD. Максимальная длина строки – 22 символа.
result	(Опционально) Укажите, чтобы удалить результаты LM.
statistics	(Опционально) Укажите, чтобы очистить статистику кадров ETH-LM (LMM и LMR).
all	Укажите, чтобы удалить информацию о CFM LM для всех MEP.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для удаления информации о функции LM.

Пример

В данном примере показано, как удалить информацию о функции LM.

```
Switch#clear cfm lm mepid 1 ma name opl domain op-domain
Switch#
```

14-32 dm enable

Данная команда используется для запуска функции DM (Delay Measurement) кадра ITU Y.1731. Используйте форму **no**, чтобы отключить данную функцию.

dm enable
no dm enable

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

CFM MEP Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения/выключения функции DM. Когда функция Frame Delay Measurement запущена на MEP от имени администратора, MEP могут генерировать информацию по временным меткам, а также отвечать на сообщения DMR, получая сообщения DMM.

Пример

В данном примере показано, как запустить функцию DM.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#cfm mep mepid 1 ma name opl domain op-domain
Switch(config-cfm-mep)#dm enable
Switch(config-cfm-mep)#
```

14-33 cfm dm test

Данная команда используется для запуска теста DM.

cfm dm test *MAC-ADDR* **mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* [**period-interval** *SELECTION*] [**percentile** *NUMBER*] [**pdu-priority** *COS-VALUE*]

Параметры

mepid <i>MEP-ID</i>	Укажите MEP ID.
name <i>MA-NAME</i>	Укажите имя МА.
domain <i>DOMAIN-NAME</i>	Укажите имя MD. Максимальная длина строки – 22 символа.
period-interval <i>SELECTION</i>	(Опционально) Укажите интервал передачи сообщений DDM и интервал диагностики: 100ms-1sec: интервал передачи – 100 миллисекунд, интервалдиагностики – 1 секунда. 1sec-10sec: интервал передачи – 1 секунда, интервал диагностики – 10 секунд (значения по умолчанию). 10sec-1min: интервал передачи – 10 секунд, интервал диагностики – 1 минута.
percentile <i>NUMBER</i>	(Опционально) Укажите процентиль измерений FD (Frame Delay) и FDV (Frame Delay Variation). Допустимый диапазон: от 0 до 100. Значение по умолчанию – 75.
pdu-priority <i>COS-VALUE</i>	(Опционально) Установите приоритет 802.1p в сообщениях DMM, передаваемых при помощи MEP. Значение по умолчанию – приоритет PDU MEP.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для запуска теста DM на MEP. MEP периодически будут отправлять сообщения DMM на удаленные MEP в пределах диагностического интервала. Система вычислит FD и FDV на основе полученных сообщений DMR и процентиля теста DM. Чтобы рассчитать FDV, необходимы непрерывно получаемые кадры DMR. Пользователь может прервать тест Frame Delay Measurement, отключив функцию Frame Delay Measurement на MEP.

Пример

В данном примере показан процесс запуска теста LM.

```
Switch# cfm dm test 00-84-57-00-00-00 mepid 1 ma name opl domain op-domain period-interval
1sec-10sec percentile 75 pdu-priority 7
Switch#
```

14-34 show cfm dm

Данная команда используется для отображения информации о DM.

```
show cfm dm [mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME]
```

Параметры

mepid <i>MEP-ID</i>	Укажите MEP ID.
name <i>MA-NAME</i>	Укажите имя MA.
domain <i>DOMAIN-NAME</i>	Укажите имя MD. Максимальная длина строки – 22 символа.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения информации DM на MEP. Если не заданы опциональные параметры, будет отображена вся информация.

Максимальное количество результатов Frame Delay Measurement, которое может храниться на устройстве – 128.

Пример

В данном примере показано, как отобразить информацию о DM.

```

Switch#show cfm dm mepid 1 ma name opl domain op-domain

MEP ID: 1
MA Name: opl
Domain Name: op-domain
State: Enabled
DMM Transmitted : 11
DMR Received   : 0
DMM Received   : 0
DMR Transmitted : 0

Period:
ID  MAC Address      Status  Interval  PCT  Pri  FD  nanosec  FDV  nanosec  Start Time
-----
1   00-84-57-00-00-00 Failed  1s:10s   75   0   0       0       0       2000-02-03
                                         00:25:06

Switch#

```

14-35 clear cfm dm

Данная команда используется для удаления информации о функции DM.

clear cfm dm {mepid *MEP-ID* ma name *MA-NAME* domain *DOMAIN-NAME* [result | statistics] | all}

Параметры

mepid <i>MEP-ID</i>	Укажите MEP ID.
name <i>MA-NAME</i>	Укажите имя MA.
domain <i>DOMAIN-NAME</i>	Укажите имя MD. Максимальная длина строки – 22 символа.
result	(Опционально) Укажите, чтобы удалить результаты DM.
statistics	(Опционально) Укажите, чтобы очистить статистику кадров ETH-DM (DMM и DMR).
all	(Опционально) Укажите, чтобы удалить информацию CFM DM для всех MEP.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для удаления информации о функции DM.

Пример

В данном примере показано, как удалить информацию о функции DM.

```
Switch#clear cfm dm mepid 1 ma name opl domain op-domain
Switch#
```

14-36 show cfm

Данная команда используется для отображения общего состояния CFM.

show cfm

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения общего состояния CFM.

Пример

В данном примере показано, как отобразить общее состояние CFM.

```
Switch#show cfm

CFM State: Enabled
AIS Trap State: Disabled
LCK Trap State: Disabled
Domain Name: op-domain           Level: 2

Switch#
```

14-37 show cfm domain

Данная команда используется для отображения информации о домене технического обслуживания CFM.

show cfm domain *DOMAIN-NAME*

Параметры

<i>DOMAIN-NAME</i>	Укажите имя домена технического обслуживания. Максимальная длина строки – 22 символа.
--------------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения информации о домене технического обслуживания CFM.

Пример

В данном примере показано, как отобразить информацию о домене технического обслуживания CFM.

```
Switch#show cfm domain op-domain
Domain Name: op-domain
Domain Level: 2
MIP Creation: Auto
SenderID TLV: Chassis
MA Name: opl
Switch#
```

14-38 show cfm ma

Данная команда используется для отображения информации о CFM MA.

show cfm ma name MA-NAME domain DOMAIN-NAME

Параметры

name MA-NAME	Укажите имя MA.
domain DOMAIN-NAME	Укажите имя MD. Максимальная длина строки – 22 символа.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения информации об ассоциации технического обслуживания CFM.

Пример

В данном примере показано, как отобразить информацию об ассоциации технического обслуживания CFM.

```
Switch#show cfm ma name opl domain op-domain

MA Name: opl
MA Mode: Software
MA VID: 2
MIP Creation: Auto
CCM Interval: 10 seconds
SenderID TLV: Chassis
MEPID List  : 1-2
  MEPID: 1  Port: 1/0/1  Direction: Up

Switch#
```

Отображаемые параметры

MEPID	MEP, уже созданная в МА.
Port	Порт MEP.
Direction	Направление MEP (Up или Down).

14-39 show cfm mep

Данная команда используется для отображения информации о MEP.

show cfm mepid *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME*

Параметры

mepid <i>MEP-ID</i>	Укажите MEP ID. Допустимый диапазон значений: от 1 до 8191.
name <i>MA-NAME</i>	Укажите имя МА.
domain <i>DOMAIN-NAME</i>	Укажите имя MD. Максимальная длина строки – 22 символа.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения информации о MEP.

Пример

В данном примере показано, как отобразить информацию о MEP.

```
Switch#show cfm mepid 1 ma name op1 domain op-domain

MEPID: 1
Mode: Software
Port: 1/0/1
Direction: Up
CFM Port Status: Enabled
MAC Address: F0-7D-68-10-21-30
MEP State: Enabled
CCM State: Disabled
PDU Priority: 7
Fault Alarm: None
Alarm Time: 250 centisecond((1/100)s)
Alarm Reset Time: 1000 centisecond((1/100)s)
Highest Fault: Some Remote MEP Down
AIS State: Disabled
AIS Period: 1 Second
AIS Client Level: Invalid
AIS Status: Not Detected
LCK State: Disabled
LCK Period: 1 Second
LCK Client Level: Invalid
LCK Status: Not Detected
LCK Action: Stop
Out-of-Sequence CCMs Received: 0
Cross-connect CCMs: 0
Error CCMs Received: 0
Port Status CCMs Received: 0
CCMs transmitted: 0
Out-of-order LBRs Received: 0
Unexpected LTRs Received: 0
AIS PDUs Received: 0
LCK PDUs Received: 0
Normal CCMs Received: 0
If Status CCMs Received: 0
In-order LBRs Received: 0
Next LTM Trans ID: 0
LBMs Transmitted: 0
AIS PDUs Transmitted: 0
LCK PDUs Transmitted: 0

Switch#
```

Отображаемые параметры

Highest Fault	<p>На данной MEP обнаружена неисправность высокого приоритета. Будет отображен один из нижеперечисленных параметров:</p> <p>None: неисправности отсутствуют с момента последнего состояния FNG_RESET.</p> <p>Some Remote MEP Defect Indication: согласно последнему CCM, полученному данной MEP от одной из удаленных MEP, удаленная MEP обнаружила неисправность.</p> <p>Some Remote MEP MAC Status Error: согласно последнему CCM, полученному данной MEP, связанный MAC удаленной MEP сообщает о наличии ошибки.</p> <p>Some Remote MEP Down: данная MEP не получает CCM от других MEP из списка конфигурации.</p> <p>Error CCM Received: данная MEP получает неверные CCM, что может быть вызвано ошибкой конфигурации.</p> <p>Cross-connect CCM Received: CCM, которые получает MEP, возможно, принадлежат другой МА.</p>
Fault Alarm	<p>На данной MEP настроена система оповещения о неисправностях. Будет отображен один из нижеперечисленных параметров:</p> <p>All: в настройках системы оповещения о неисправностях выбран режим «all».</p> <p>MAC Status: в настройках системы оповещения о неисправностях выбран режим «mac-status».</p> <p>Remote CCM: в настройках системы оповещения о неисправностях выбран режим «remote-ccm».</p> <p>Error CCM: в настройках системы оповещения о неисправностях выбран режим «error-ccm».</p> <p>Xcon CCM: в настройках системы оповещения о неисправностях выбран режим «xcon-ccm».</p> <p>None: в настройках системы оповещения о неисправностях выбран режим «none».</p>

14-40 show cfm interface

Данная команда используется для отображения информации о CFM на указанном физическом интерфейсе.

```
show cfm interface [INTERFACE-ID [, | -]]
```

Параметры

Interface <i>INTERFACE-ID</i>	(Опционально) Укажите ID интерфейса, который необходимо отобразить. Применимо только для физических интерфейсов.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса

недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения информации о CFM на указанных физических портах.

Пример

В данном примере показано, как отобразить информацию о CFM на указанных физических портах.

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

eth1/0/1
CFM is enabled
MAC Address: F0-7D-68-10-21-30

  Domain Name: op-domain
  Level: 2
  MA Name: op1
  VID: 2
  MEPID: 1
  Direction: Up

Switch#
```

14-41 show cfm remote-mep

Данная команда используется для отображения информации об удаленных MEP.

```
show cfm remote-mep mepid LOCAL-MEP-ID ma name MA-NAME domain DOMAIN-NAME
[remote-mepid REMOTE-MEPID]
```

Параметры

mepid LOCAL-MEP-ID	Укажите MEP ID.
name MA-NAME	Укажите имя MA.
domain DOMAIN-NAME	Укажите имя MD. Максимальная длина строки – 22 символа.
remote-mepid	(Опционально) Укажите ID удаленной MEP. Допустимый

REMOTE-MEPID	диапазон: от 1 до 8191. Если значение не задано, будут отображены все удаленные MEP.
---------------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения информации об удаленных MEP.

Пример

В данном примере показано, как отобразить информацию об удаленных MEP, доступную локальной MEP 1.

```
Switch#show cfm remote-mep mepid 1 ma name opl domain op-domain

Remote MEPID: 2
MAC Address: FF-FF-FF-FF-FF-FF
Status: OK           RDI: Yes
Port State: Up       Interface Status: No
Last CCM Serial Number: 1000
Sender Chassis ID: None
Sender Management Address: SNMP-UDP-IPv4 10.90.90.90:161
Detect Time: 2000-02-02 23:21:38

Remote MEPID: 3
MAC Address: 11-22-33-44-02-05
Status: OK           RDI: Yes
Port State: Up       Interface Status: No
Last CCM Serial Number: 200
Sender Chassis ID: None
Sender Management Address: SNMP-UDP-IPv4 10.90.90.90:161
Detect Time: 2010-11-01 17:00:00

Switch#
```

В данном примере показано, как отобразить информацию об удаленной MEP.

```
Switch# show cfm remote-mep mepid 1 ma name op-ma domain op-domain remote-mepid 2

Remote MEPID: 2
MAC Address: FF-FF-FF-FF-FF-FF
Status: OK                RDI: Yes
Port State: Up           Interface Status: No
Last CCM Serial Number: 1000
Sender Chassis ID: None
Sender Management Address: SNMP-UDP-IPv4 10.90.90.90:161
Detect Time: 2000-02-02 23:21:38

Switch#
```

Отображаемые параметры

Status	<p>Отображает режим работы диаграммы состояний удаленной MEP:</p> <p>IDLE: выполняется перезапуск.</p> <p>START: таймер не истек с момента перезапуска диаграммы состояний итеперь является недействительным. CCM получен.</p> <p>FAILED: таймер истек с момента получения действительного CCM или смоента перезапуска диаграммы состояний.</p> <p>OK: действительный CCM получен до момента истечения таймера.</p>
RDI	<p>Отображает наличие/отсутствие бита RDI в последнем полученном CCM:</p> <p>Yes: бит RDI установлен.</p> <p>No: бит RDI удален / действительные CCM не получены.</p>
Port State	<p>Указывает, может ли порт моста, на котором находится удаленная MEP, пропускать простые данные независимо от статуса MAC:</p> <p>None: CCM не получен / в последнем полученном CCM отсутствует TLV статуса порта.</p> <p>Blocked: простые данные не могут свободно поступать через порт, на котором присутствует удаленная MEP.</p> <p>Up: простые данные могут свободно поступать через порт, на котором присутствует удаленная MEP.</p>
Interface Status	<p>Отображает статус интерфейса, на котором настроена удаленная MEP, передающая CCM (этим интерфейсом может являться не только тот интерфейс, на котором присутствует данная MEP) или статус следующего интерфейса ниже в IETF RFC 2863 IF-MIB.</p> <p>None: CCM не получены / в последнем полученном CCM отсутствует TLV статуса интерфейса.</p> <p>Up: интерфейс готов к передаче пакетов.</p> <p>Down: передача пакетов на данном интерфейсе невозможна.</p> <p>Testing: тестовый режим интерфейса.</p> <p>Unknown: невозможно определить статус интерфейса.</p> <p>Dormant: передача пакетов на данном интерфейсе</p>

невозможна, интерфейс находится в режиме ожидания внешнего события.

Notpresent: отсутствует один из компонентов интерфейса.

Lowerlayerdown: интерфейс отключен из-за состояния интерфейсов нижнего слоя.

14-42 show cfm mep fault

Данная команда используется для отображения MEP, у которых обнаружены неисправности.

show cfm mep fault

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для получения сведений о состоянии отказа MEP. Команда отображает все неисправности, обнаруженные на MEP.

Пример

В данном примере показано, как отобразить MEP, имеющие неисправности.


```
Switch# show cfm mep fault

Domain Name: md5
MA Name: ma5
MEPID: 2
Status: Some Remote MEP Down
AIS Status: Normal
LCK Status: Normal

Domain Name: md6
MA Name: ma6
MEPID: 3
Status: Some Remote MEP Down
AIS Status: Normal
LCK Status: Normal

Switch#
```

Отображаемые параметры

Status	<p>На MEP обнаружена неисправность высокого приоритета, будет отображен один из нижеперечисленных параметров:</p> <p>None: неисправности отсутствуют с момента последнего состояния FNG_RESET.</p> <p>Some Remote MEP Defect Indication: согласно последнему CCM, полученному данной MEP от одной из удаленных MEP, удаленная MEP обнаружила неисправность.</p> <p>Some Remote MEP MAC Status Error: согласно последнему CCM, полученному данной MEP, ассоциированный MAC удаленной MEP сообщает о состоянии отказа.</p> <p>Some Remote MEP Down: данная MEP не получает CCM от других MEP из списка конфигурации.</p> <p>Error CCM Received: данная MEP получает неисправные CCM, что может быть вызвано ошибкой конфигурации.</p> <p>Cross-connect CCM Received: CCM, которые получает MEP, возможно, принадлежат другой MA.</p>
AIS Status	<p>AIS Detected: AIS PDU получены.</p> <p>Normal: AIS PDU не получены.</p>
LCK Status	<p>LCK Detected: LCK PDU получены.</p> <p>Normal: LCK PDU не получены.</p>

14-43 show cfm mip ccm

Данная команда используется для отображения записей базы данных MIP CCM.

```
show cfm mip ccm
```

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения записей базы данных MIP CCM.

Пример

В данном примере показано, как отобразить записи базы данных MIP CCM.

```
Switch# show cfm mip ccm

VID: 10
MAC Address: 00-07-00-00-00-1C
Port: eth1/0/12

VID: 10
MAC Address: 00-07-00-00-00-1E
Port: eth1/0/14

Total: 2

Switch#
```

14-44 show cfm pkt-cnt interface

Данная команда используется для отображения счетчиков RX/TX пакета CFM указанного физического интерфейса.

show cfm pkt-cnt interface [INTERFACE-ID [, | -]] [rx] [tx]

Параметры

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

rx	(Опционально) Используется для обозначения счетчиков RX указанного физического интерфейса.
tx	(Опционально) Используется для обозначения счетчиков TX указанного физического интерфейса.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения счетчиков пакета физического интерфейса. Если интерфейсы не указаны, будут отображены счетчики всех интерфейсов. Если указан только физический интерфейс, будут отображены счетчики пакетов RX и TX. Если указан только тип RX или TX, будут отображены счетчики пакета RX или TX всех физических интерфейсов.

Пример

В данном примере показано, как отобразить счетчики пакета Ethernet 1/0/1.

```
Switch#show cfm pkt-cnt interface ethernet 1/0/1

eth1/0/1
  CFM RX Statistics
    AllPkt:0      CCM:0
    LBR:0         LBM:0
    LTR:0         LTM:0
    VidDrop:0     OpcoDrop:0
  CFM TX Statistics
    AllPkt:0      CCM:0
    LBR:0         LBM:0
    LTR:0         LTM:0

Switch#
```

В данном примере показано, как отобразить счетчики пакета RX Ethernet 1/0/1.

```
Switch#show cfm pkt-cnt interface ethernet 1/0/1 rx

eth1/0/1
  CFM RX Statistics
  AllPkt:0          CCM:0
  LBR:0             LBM:0
  LTR:0             LTM:0
  VidDrop:0         OpcoDrop:0

Switch#
```

В данном примере показано, как отобразить счетчики пакета TX Ethernet 1/0/1.

```
Switch#show cfm pkt-cnt interface ethernet 1/0/1 tx

eth1/0/1
  CFM TX Statistics
  AllPkt:0          CCM:0
  LBR:0             LBM:0
  LTR:0             LTM:0

Switch#
```

Отображаемые параметры

VidDrop	Пакеты отбрасываются из VLAN.
OpcoDrop	Пакеты отбрасываются при несоответствии нормальному ор- code.

14-45 clear cfm pkt-cnt interface

Данная команда используется для обнуления счетчиков RX/TX пакета CFM указанного физического интерфейса.

```
clear cfm pkt-cnt interface {INTERFACE-ID [, | -] | all} [rx] [tx]
```

Параметры

<i>INTERFACE-ID</i>	Укажите ID интерфейса, который необходимо удалить. Применимо только для физических интерфейсов.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
all	Укажите, чтобы обнулить все счетчики CFM интерфейса.
rx	(Опционально) Используется для обозначения счетчиков RX указанного физического интерфейса.
tx	(Опционально) Используется для обозначения счетчиков TX указанного физического интерфейса.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для обнуления счетчиков пакета физического интерфейса. Если указан только физический интерфейс, будут обнулены счетчики пакетов RX и TX указанного физического интерфейса. Если указаны физический интерфейс и тип RX/TX, будут обнулены счетчики пакета RX или TX указанного физического интерфейса.

Пример

В данном примере показано, как обнулить счетчики пакета TX Ethernet 1/0/1.

```
Switch# clear cfm pkt-cnt interface ethernet 1/0/1 tx
Switch#
```

14-46 cfm mp-ltr-all

Данная команда используется для настройки всех MP так, чтобы они отвечали сообщением LTR. Используйте форму **no**, чтобы отключить данную функцию.

```
cfm mp-ltr-all
no cfm mp-ltr-all
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

В соответствии с IEEE 802.1ag мост отправляет LTR в ответ на LTM. Используйте данную команду, чтобы все MP на канале перенаправления LTM отправляли LTR, вне зависимости от того, находятся ли они на том же мосту.

Пример

В данном примере показано, как запустить данную функцию.

```
Switch# configure terminal
Switch(config)# cfm mp-ltr-all
Switch(config)#
```

14-47 show cfm mp-ltr-all

Данная команда используется для отображения конфигурации ответов MP на LTR.

show cfm mp-ltr-all

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения конфигурации ответов MP на LTR.

Пример

В данном примере показано, как отобразить конфигурацию ответов MP на LTR.

```
Switch# show cfm mp-ltr-all

All MPs reply LTRs: Disabled

Switch#
```

15. Команды CPU Access Control List (ACL)

15-1 soft-acl filter-map

Данная команда используется для создания или изменения программных списков управления доступом (Software ACL Filter Map). Данная команда влечет вход в режим настройки Software ACL Filter Map Configuration Mode. Используйте форму **no** для удаления программных списков управления доступом (Software ACL Filter Map).

```
soft-acl filter-map NAME
no soft-acl filter-map NAME
```

Параметры

<i>NAME</i>	Имя программного списка управления доступом (Software ACL FilterMap), которой должен быть настроен. Длина имени не должна превышать 32 символов.
-------------	--

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для входа в режим настройки Software ACL Filter Map Configuration Mode, а также для связывания нескольких предварительно заданных ACL для фильтрации пакетов, получаемых CPU. Можно настроить несколько программных списков управления доступом (Software ACL Filter Map).

Пример

В данном примере показано, как создать программный список управления доступом (Software ACL Filter Map) с именем «cpu_filter».

```
Switch# configure terminal
Switch(config)# soft-acl filter-map cpu_filter
Switch(config-soft-acl)#
```

15-2 match access-group

Данная команда используется для связи списка доступа с программным списком управления доступом (Software ACL Filter Map). Используйте форму **no** для удаления привязки.

```
SEQUENCE-NUMBER match mac access-group NAME
SEQUENCE-NUMBER match ip access-group NAME
```

SEQUENCE-NUMBER match ipv6 access-group NAME
no match {mac | ip | ipv6} access-group

Параметры

<i>SEQUENCE-NUMBER</i>	Порядковый номер соответствующей записи совпадения. Диапазон: от 1 до 65535. Чем меньше номер, тем выше приоритет списка доступа.
<i>NAME</i>	Указывает имя списка доступа ACL, которое должно совпадать.

По умолчанию

Нет

Режим ввода команды

Software ACL Filter Map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для привязки списка доступа с программным списком управления доступом (Software ACL Filter Map). Несколько списков доступа могут быть связаны с программным списком управления доступом (Software ACL Filter Map). Однако они должны быть разных типов (expert, MAC, IP и IPv6). Когда связан список доступа одинакового типа, каждая последующая команда перезаписывает предыдущую команду.

Порядковые номера определяют приоритет обработки связанного списка доступа в Filter Map. Список доступа с меньшим порядковым номером обладает более высоким приоритетом. Если существуют связанные списки доступа с одинаковым порядковым номером, они обрабатываются в следующем порядке: список доступа expert, список доступа MAC, список доступа IP, список доступа IPv6.

Пример

В данном примере показано, как привязать список доступа IP с именем «cpu-acl» и список доступа MAC с именем mac4001 к программному списку управления доступом (Software ACL Filter Map) «cpu_filter».

```
Switch# configure terminal
Switch(config)# ip access-list cpu-acl
Switch(config-ip-acl)# permit 10.20.0.0 255.255.0.0
Switch(config-ip-acl)# exit
Switch(config)# mac access-list extended mac4001
Switch(config-mac-ext-acl)# 25 deny host 0013.0049.8272 any
Switch(config-mac-ext-acl)# exit
Switch(config)# soft-acl filter-map cpu_filter
Switch(config-soft-acl)# 2 match ip access-group cpu-acl
Switch(config-soft-acl)# 3 match mac access-group mac4001
Switch(config-soft-acl)#
```

15-3 match interface

Данная команда используется для настройки соответствующих входных интерфейсов. Используйте форму **no** для удаления соответствующих входных интерфейсов.

```
match interface INTERFACE-ID [, | -]
no match interface {all | INTERFACE-ID [, | -]}
```

Параметры

<i>INTERFACE-ID</i>	Соответствующий идентификатор интерфейса (Interface ID). Корректными интерфейсами являются физические интерфейсы.
,	(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.
all	Указывает в форме no этой команды удалить все совместимые входные интерфейсы.

По умолчанию

Нет

Режим ввода команды

Software ACL Filter Map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Программный список управления доступом (Software ACL Filter Map) будет активирован, когда настроен один или несколько совместимых интерфейсов. Другими словами, если совместимый интерфейс не настроен, программный список не вступит в силу.

Когда пакет принимается CPU и входной интерфейс настроен на программном списке управления доступом (Software ACL Filter Map), коммутатор будет автоматически выполнять поиск связанных списков доступа соответствующего списка.

Связанный список доступа с наивысшим приоритетом в программном списке будет проверен в первую очередь. Когда совпадение будет обнаружено, другие списки доступа будут проигнорированы. В противном случае, будет выполняться поиск списка доступа со следующим наивысшим приоритетом и так далее.

Внутри списка доступа используется похожая проверка номеров. Правило с меньшим порядковым номером получает более высокий приоритет. Когда совпадение будет обнаружено, другие будут проигнорированы.

В итоге, если совпадение не обнаружено, пакет будет разрешен, и он может непрерывно обрабатываться другими функциями.

Если действием является 'permit', он будет пропущен к другим функциям. Если действием является 'drop', пакет будет отброшен.

Другими словами, действие программного списка основано на точно настроенной записи «разрешить/запретить». Пакет разрешен, если он не соответствует какому-либо точному правилу «разрешить» или «запретить».

Интерфейс может принадлежать не более чем одному списку. Когда интерфейс настроен для нового программного списка, он будет удален из предыдущего списка.

Пример

В данном примере показано, как настроить совместимый интерфейс Ethernet 1/0/1 для программного списка управления доступом (Software ACL Filter Map) «cpu_filter».

```
Switch# configure terminal
Switch(config)# ip access-list cpu-acl
Switch(config-ip-acl)# permit 10.20.0.0 0.0.255.255
Switch(config-ip-acl)# exit
Switch(config)# mac access-list extended mac4001
Switch(config-mac-ext-acl)# 25 deny host 0013.0049.8272 any
Switch(config-mac-ext-acl)# exit
Switch(config)# soft-acl filter-map cpu_filter
Switch(config-soft-acl)# 2 match ip access-group cpu-acl
Switch(config-soft-acl)# 3 match mac access-group mac4001
Switch(config-soft-acl)# match interface ethernet 1/0/1
Switch(config-soft-acl)#
```

15-4 show soft-acl

Данная команда используется для отображения информации о программном списке управления доступом (Software ACL Filter Map).

show soft-acl filter-map [NAME]

Параметры

<i>NAME</i>	(Опционально) Указывает имя отображаемого программного списка управления доступом (Software ACL Filter Map).
-------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду для отображения указанного программного списка управления доступом (Software ACL Filter Map). Если имя не указано, то будут отображаться все списки.

Пример

В данном примере показано, как отобразить программный список управления доступом (Software ACL Filter Map).

```
Switch# show soft-acl filter-map

Software ACL Filter Map
  cpu_filter:
Match Access-list(s):
  IP(2): Ext-ip
  MAC(3):mac4001
Match Ingress Interface(s):
  eth1/0/1

Switch#
```

Отображаемые параметры

IP(N)	Тип списка доступа. Число в скобках означает порядковый номер связанного списка доступа.
--------------	--

16. Команды Debug

16-1 debug enable

Данная команда используется для включения функции вывода сообщения отладки (Debug). Используйте форму **no** для отключения данной функции.

```
debug enable
no debug enable
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для включения функции вывода сообщения отладки (Debug).

Пример

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

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

16-2 debug output

Используйте данную команду, чтобы обозначить индивидуальные модули, для которых необходимо вывести сообщение отладки (Debug). Используйте форму **no**, чтобы отключить данную функцию.

```
debug output {module MODULE-LIST | all} {buffer | console}
no debug output {module MODULE-LIST | all}
```

Параметры

MODULE-LIST

Укажите список модулей, для которых необходимо вывести сообщение отладки (Debug). Отделяйте названия модулей

	при помощи пробелов.
all	Укажите, чтобы вывести сообщение отладки (Debug) всех модулей в указанный пункт назначения.
buffer	Укажите, чтобы вывести сообщение отладки (Debug) в буфер отладки.
console	Укажите, чтобы вывести сообщение отладки (Debug) на локальную консоль.

По умолчанию

По умолчанию сообщение отладки (Debug) выводится в буфер.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для вывода сообщения отладки (Debug) указанного модуля в буфер или на локальную консоль. Используйте команду **debug show output** для отображения информации о строке модуля. По умолчанию сообщение отладки (Debug) модуля выводится в буфер отладки. Для вывода сообщения отладки (Debug) модуля необходимо запустить настройки отладки модуля, а также запустить команду отладки (Debug) в общем режиме.

Пример

В данном примере показано, как вывести все сообщения отладки (Debug) модуля в буфер отладки.

```
Switch# debug output all buffer
Switch#
```

16-3 debug reboot on-error

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

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

Параметры

Нет

По умолчанию

По умолчанию данный режим включен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

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

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

16-4 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

<i>SOURCE-URL</i>	Укажите ссылку на файл, который необходимо скопировать: buffer: укажите, чтобы скопировать данные буфера отладки. error-log: укажите, чтобы скопировать данные журнала регистрации ошибок. tech-support: укажите, чтобы скопировать справочную техническую информацию.
<i>LOCATION</i>	Укажите адрес IPv4 или IPv6 TFTP-сервера.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

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

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

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

Switch#
```

16-5 debug clear buffer

Данная команда используется для очистки буфера отладки.

debug clear buffer

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для очистки буфера отладки.

Пример

В данном примере показано, как очистить буфер отладки.

```
Switch# debug clear buffer
Switch#
```

16-6 debug clear error-log

Данная команда используется для очистки журнала регистрации ошибок.

debug clear error-log

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для очистки журнала регистрации ошибок.

Пример

В данном примере показано, как очистить журнал регистрации ошибок.

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

16-7 debug show buffer

Данная команда используется для отображения содержимого буфера отладки или информации по его эксплуатации.

debug show buffer [utilization]

Параметры

utilization	(Опционально) Укажите, чтобы отобразить информацию по эксплуатации буфера отладки.
--------------------	--

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для отображения содержимого буфера отладки или информации по его эксплуатации. Если не указаны опциональные параметры, будет отображено содержимое буфера.

Пример

В данном примере показано, как отобразить данные буфера отладки.

```
Switch# debug show buffer  
  
Debug buffer is empty  
  
Switch#
```

В данном примере показано, как отобразить информацию по эксплуатации буфера отладки.

```
Switch# debug show buffer utilization  
  
Debug buffer is allocated from system memory  
Total size is 2M  
Utilization is 30%  
  
Switch#
```

16-8 debug show output

Данная команда используется для отображения статуса отладки и вывода информации о модулях.

debug show output

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для отображения информации о выводе статуса отладки и сообщения отладки (Debug) модулей.

Пример

В данном примере показано, как отобразить информацию о выводе сообщения отладки (Debug) модулей.

```
Switch#debug show output

Debug Global State : Disabled

Module name      Output      Enabled
-----
MSTP             buffer     No
VRRP             buffer     No
RIPNG            buffer     No

Switch#
```

16-9 debug show error-log

Данная команда используется для отображения данных журнала регистрации ошибок.

debug show error-log

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для отображения данных журнала регистрации ошибок.

Пример

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

```
Switch# debug show error log

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

Current TASK : bcmARL.0
----- TASK STACKTRACE -----
->802ACE98
->8018C814
->8028FF44
->8028352C
->801D703C
->8013B8A4
->802AE754
->802A5E0C
->802A5D6C
.....
# debug log: 2
# level: fatal
# clock: 10000ms
# time : 2013/03/11 15:00:00
***** SOFTWARE FATAL ERROR *****
CLI_UTL_AllocateMemory Fail!

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

Total Log : 2

Switch#
```

16- 10 debug show tech-support

Данная команда используется для отображения информации, запрашиваемой техническим персоналом.

debug show tech-support

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 15

Использование команды

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

Пример

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

```
Switch#debug show tech-support

#-----
#                               DGS-3130-30TS Gigabit Ethernet Switch
#                               Technical Support Information
#
#                               Firmware: Build 1.00.001
#                               Copyright (C) 2017 D-Link Corporation. All rights reserved.
#-----

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

[SYS 2015-12-14 13:45:29]

Boot Time       : 14 Dec 2015 08:22:59
RTC Time        : 2015/12/14 13:45:29
Boot PROM Version : Build 1.00.001
Firmware Version : Build 1.00.001
Hardware Version : A1
Serial number    : DGS3130102030
MAC Address      : F0-7D-68-36-30-00
MAC Address Number : 65535

PacketType      TotalCounter   Pkt/Sec  PacketType      TotalCounter   Pkt/Sec
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

16-11 debug show cpu utilization

Данная команда используется для отображения полного коэффициента загрузки CPU, а также коэффициента загрузки CPU с разбивкой на процессы.

debug show cpu utilization

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы отобразить информацию по загрузке CPU и загрузке по каждому процессу.

Пример

В данном примере показано, как отобразить информацию о загрузке CPU с разбивкой на процессы.

```
Switch#debug show cpu utilization

Five seconds - 22 %          One minute - 20 %          Five minutes - 20 %

Process Name                5Sec      1Min      5Min
-----
tIdleTask0                  78 %      80 %      80 %
bcmCNTR.0                   9 %       8 %       9 %
bcmL2X.0                     7 %       5 %       5 %
bcmMEM_SCAN.0               0 %       0 %       0 %
hisr1                        0 %       0 %       0 %
NICRX                        0 %       0 %       0 %
cpuprotect                   0 %       0 %       0 %
MAUMIB_TASK                  0 %       0 %       0 %
bcmLINK.0                    0 %       0 %       0 %
socdmadesc.0                 0 %       0 %       0 %
bcmRX                         0 %       0 %       0 %
bcmIbodSync.0                0 %       0 %       0 %
8021xCtrl                    0 %       0 %       0 %
radius_reader                 0 %       0 %       0 %
CLI                           0 %       0 %       0 %
OS_TIMER                      0 %       0 %       0 %
CNT_TASK                      0 %       0 %       0 %
historcnt_task                0 %       0 %       0 %
EEE_LLDPTask                  0 %       0 %       0 %
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

17. Команды DHCP Auto-Configuration

17-1 autoconfig enable

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

```
autoconfig enable
no autoconfig enable
```

Параметры

Нет

По умолчанию

По умолчанию данная функция выключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

- Коммутатор получает путь к файлу конфигурации, а также IP-адрес TFTP-сервера от DHCP-сервера (при наличии этих данных у DHCP-сервера, а также если в настройках указано, что DHCP-сервер может передавать данную информацию в поле данных пакета DHCP-ответа).
- Коммутатор загружает файл конфигурации, полученный от TFTP-сервера (если TFTP-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
Warning:Autoconfig enabled on VLAN 1 now, but won't take effect until reboot.
Switch(config)#
```

17-2 show autoconfig

Данная команда используется для отображения статуса автоконфигурации.

show autoconfig

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения статуса автоконфигурации.

Пример

В данном примере показано, как отобразить статус автоконфигурации.

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

18. Команды DHCP Client

18-1 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

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

18-2 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

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

18-3 ip dhcp client hostname

Используйте данную команду, чтобы указать значение опции имени узла (Host Name) для отправки в сообщении DHCP Discover. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip dhcp client hostname HOST-NAME  
no ip dhcp client hostname
```

Параметры

<i>HOST-NAME</i>	Укажите имя узла. Максимальная длина строки – 64 символа. Имя узла должно начинаться с буквы, заканчиваться буквой или точкой, внутри можно использовать буквы, точки и дефисы.
------------------	---

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать строку имени узла (Option 12) для отправки в сообщении DHCP Discover. Данная функция применяется только для последующей отправки сообщений DHCP Discover. Данная функция работает, когда на интерфейсе включен DHCP-клиент, который может получить IP-адрес от DHCP-сервера. Если данная функция не настроена, коммутатор будет отправлять сообщения без Option 12.

Пример

В данном примере показано, как установить значение опции имени узла (Host Name). Указанное значение – Site-A-Switch.

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

18-4 ip dhcp client lease

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

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

Параметры

<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

Уровень команды по умолчанию

Уровень 12

Использование команды

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

Пример

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

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

19. Команды DHCP Relay

19-1 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

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

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Наряду с пакетами DHCP Relay, подчиняющимися команде **ip helper-address**, Relay Destination DHCP-сервера можно указать в пуле DHCP Relay. Для этого войдите в режим настройки пула 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)#
```

19-2 ip dhcp relay information check

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

ip dhcp relay information check
no ip dhcp relay information check

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применима, если включен сервис DHCP.

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

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

Если функция Check отключена, пакет будет передан напрямую.

Пример

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

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

19-3 ip dhcp relay information check-reply

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

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

Параметры

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

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применима, если включен сервис DHCP.

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

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

Если проверка отключена, пакет будет передан напрямую.

Пример

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

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

19-4 ip dhcp relay information option

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

ip dhcp relay information option
no ip dhcp relay information option

Параметры

Нет

По умолчанию

По умолчанию Option 82 не встроена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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

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

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

Пример

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

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

19-5 ip dhcp relay information option-insert

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

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

Параметры

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

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применима, если запущена команда **service dhcp**.

Пример

В данном примере показано, как включить функцию встраивания Option 82 в ретранслируемые пакеты DHCP-ответа и выключить данную функцию для интерфейса VLAN 100. Функция встраивания Option 82 выключена для VLAN 100, но включена для оставшихся интерфейсов.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# interface vlan 100
Switch(config-if)# ip dhcp relay information option-insert none
Switch(config-if)#
```

19-6 ip dhcp relay information policy

Данная команда используется для настройки алгоритма перенаправления Option 82 для DHCP Relay Agent. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

**ip dhcp relay information policy {drop | keep | replace}
no ip dhcp relay information policy**

Параметры

drop	Укажите, чтобы отбросить пакет, у которого уже есть Relay Option.
keep	Укажите, чтобы напрямую в неизменном виде отправить пакет DHCP-запросов, у которого уже есть Relay Option, на DHCP-сервер.

replace	Укажите, чтобы заменить пакет DHCP-запросов, у которого уже есть Relay Option, новой опцией.
----------------	--

По умолчанию

Параметр по умолчанию – **replace**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применима, если включен сервис DHCP. Используйте данную команду для настройки общего алгоритма встраивания Option 82 в пакеты, уже имеющие Option 82.

Пример

В данном примере показано, как настроить алгоритм перенаправления Relay Agent Option (Option 82) с помощью параметра **keep**. Если команда **ip dhcp relay information relay** сконфигурирована в режиме Global Configuration Mode, но не сконфигурирована в режиме Interface Configuration Mode, для всех интерфейсов применим режим Global Configuration Mode.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information policy keep
Switch(config)#
```

19-7 ip dhcp relay information policy-action

Данная команда используется для настройки алгоритма перенаправления Option 82 для DHCP Relay Agent на интерфейсе. Используйте форму **no**, чтобы удалить настройки.

ip dhcp relay information policy-action {drop | keep | replace}
no ip dhcp relay information policy-action

Параметры

drop	Укажите, чтобы отбросить пакет, у которого уже есть Relay Option.
keep	Укажите, чтобы в неизменном виде отправить пакет DHCP-запросов, у которого уже есть Relay Option, напрямую на DHCP-сервер.
replace	Укажите, чтобы заменить пакет DHCP-запросов, у которого уже есть Relay Option, новой опцией.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применима, если запущен сервис DHCP. Используйте данную команду, чтобы настроить алгоритм встраивания Option 82 на интерфейсе в пакеты, у которых уже есть Option 82.

Пример

В данном примере показано, как настроить алгоритм перенаправления Relay Agent Option с помощью параметра `keep`, а также как настроить соответствующий алгоритм для VLAN 100 с помощью параметра `drop`. Для VLAN 100 эффективным алгоритмом перенаправления Relay Agent Option является `drop`, для других интерфейсов – `keep`.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information policy keep
Switch(config)# interface vlan 100
Switch(config-if)# ip dhcp relay information policy-action drop
Switch(config-if)#
```

19-8 ip dhcp relay information option format remote-id

Данная команда используется для настройки sub-опции Remote ID DHCP. Используйте форму `no`, чтобы применить настройки по умолчанию.

**ip dhcp relay information option format remote-id {default | string SENTENCE | vendor2 | udf}
expert-no ip dhcp relay information option format remote-id**

Параметры

default

Укажите, чтобы использовать системный MAC-адрес коммутатора в качестве Remote ID. Формат Remote ID представлен ниже:

```
-----|
| a.   | b.   | c.   | d.   | e.   |
|-----|
| 2    | 8    | 0    | 6    | MAC Address |
|-----|
| 1 byte | 1 byte | 1 byte | 1 byte | 6 bytes |
|-----|
```

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.

expert-udf

Укажите, чтобы использовать expert-udf. Оригинальный формат Remote ID представлен ниже:

```

-----|
| a.    | b.    | c.    |
-----|
| 2     | n     | User Defined
-----|
| 1 byte| 1 byte| Max. 251 bytes
-----|

```

- a. Tun sub-опции:** число 2 свидетельствует о том, что тип данного ID – Remote ID.
- b. Длина:** общая длина строки, задаваемой пользователем. По умолчанию длина равна 0, поле значений отсутствует.
- c. Значение:** универсальная задаваемая пользователем строка, настраиваемая при помощи данной команды, а также команды **ip dhcp relay information profile**. Максимальная длина строки – 251 символ.

По умолчанию

По умолчанию в качестве строки Remote ID используется системный MAC-адрес коммутатора.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для выбора различных vendor-ов или заданной пользователем строки ASCII в качестве Remote ID.

Пример

В данном примере показано, как настроить vendor2 в качестве Remote ID.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format remote-id vendor2
Switch(config)#
```

В данном примере показано, как настроить в качестве Remote ID строку, задаваемую пользователем. В примере используется строка «switch1».

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format remote-id string switch1
Switch(config)#
```

19-9 ip dhcp relay information option format-type remote-id

Данная команда используется для настройки sub-опции Remote ID DHCP как строки формата vendor в режиме Interface Configuration Mode. Используйте форму **no**, чтобы удалить sub-опцию Remote ID как строку формата vendor.

```
ip dhcp relay information option format-type remote-id expert-udf NAME
no ip dhcp relay information option format-type remote-id
```

Параметры

expert-udf	Укажите Remote ID для конкретных портов, которые необходимо связать с указанным профилем Option 82. Максимально допустимое количество символов – 32.
NAME	Укажите имя профиля.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применима для настройки интерфейсов физического порта и интерфейсов port-channel. Используйте данную команду для настройки строки, определенной как vendor для sub-опции Remote ID Option 82 на интерфейсе.

Пример

В данном примере показано, как настроить строку формата expert UDF Remote ID для Ethernet 1/0/1. В примере используется строка «switch1».

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ip dhcp relay information option format-type remote-id expert-udf switch1
Switch(config-if)#
```

19-10 ip dhcp relay information option format circuit-id

Данная команда используется для настройки sub-опции Circuit ID DHCP. Используйте форму **no**, чтобы применить настройки по умолчанию.

**ip dhcp relay information option format circuit-id {default | string SENTENCE | vendor1 | udf}
expert-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, для стекированных коммутаторов – Unit ID.
- 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.

expert-udf

Укажите, чтобы использовать expert-udf. Circuit ID задается пользователем в следующем формате:

a.	b.	c.
1	n	User defined
1 byte	1 byte	Max. 251 bytes

- a. *Tun sub-опции*: число 1 свидетельствует о том, что типданного ID – Circuit ID.
- b. *Длина*: общая длина строки, задаваемой пользователем.По

умолчанию длина равна 0, поле значений отсутствует.

с. Значение: универсальная задаваемая пользователем строка, настраиваемая при помощи данной команды, а также команды **ip dhcp relay information profile**. Максимальная длина строки – 251 символ.

По умолчанию

По умолчанию форматом Circuit ID являются ID VLAN, номер модуля и номер порта.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для выбора различных vendor-ов или заданной пользователем строки ASCII в качестве Circuit ID.

Пример

В данном примере показано, как использовать vendor1 в качестве Circuit ID.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format circuit-id vendor1
Switch(config)#
```

В данном примере показано, как настроить в качестве Circuit ID строку, задаваемую пользователем. В примере используется строка «abcd».

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format circuit-id string abcd
Switch(config)#
```

19-11 ip dhcp relay information option format-type circuit-id

Данная команда используется для настройки sub-опции Circuit ID DHCP. Используйте форму **no**, чтобы удалить sub-опцию Circuit ID.

```
ip dhcp relay information option format-type circuit-id expert-udf NAME
no ip dhcp relay information option format-type circuit-id
```

Параметры

expert-udf	Укажите Circuit ID для конкретных портов, которые необходимо связать с указанным профилем Option 82. Максимально допустимое количество символов – 32.
-------------------	--

NAME	Укажите имя профиля.
------	----------------------

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и интерфейсов port-channel. Используйте данную команду для настройки строки, определенной как vendor для sub-опции Circuit ID Option 82 на интерфейсе.

Пример

В данном примере показано, как настроить expert UDF Circuit ID для ethernet 1/0/1. В примере использован expert UDF Circuit ID «abc».

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ip dhcp relay information option format-type circuit-id expert-udf abc
Switch(config-if)#
```

19-12 ip dhcp relay information trust-all

Данная команда позволяет назначить на DHCP Relay Agent все интерфейсы, отправляющие информацию об IP DHCP Relay, доверенными. Используйте форму **no**, чтобы отключить функцию Trust для всех интерфейсов.

```
ip dhcp relay information trust-all
no ip dhcp relay information trust-all
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если на интерфейсе включена опция Trust для информации IP DHCP Relay, будут приниматься пакеты, GIADDR которых равен 0 (данный Relay Agent является первой ретрансляцией данного пакета DHCP-запроса), но у которых присутствует Relay Agent Information Option (Option 82). Если интерфейс не является доверенным, пакеты будут отброшены.

Если применены настройки данной команды, информация IP DHCP Relay является доверенной со всех интерфейсов. Если настройки данной команды не применены, статус информации определяется командой **ip dhcp relay information trusted** в режиме интерфейса.

Проверить настройки можно при помощи команды **show ip dhcp relay information trusted-sources**.

Пример

В данном примере показано, как назначить на DHCP Relay Agent информацию IP DHCP Relay в качестве доверенной со всех интерфейсов. Информация Relay считается доверенной со всехинтерфейсов, вне зависимости от настроек команды **ip dhcp relay information trusted**.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information trust-all
Switch(config)#
```

19-13 ip dhcp relay information trusted

Данная команда позволяет назначить на DHCP Relay Agent определенный интерфейс, отправляющий информацию об IP DHCP Relay, в качестве доверенного. Используйте форму **no**, чтобы отключить функцию Trust для интерфейса.

```
ip dhcp relay information trusted
no ip dhcp relay information trusted
```

Параметры

Нет

По умолчанию

По умолчанию информация не является доверенной.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если информация IP DHCP Relay отправляется с доверенного интерфейса, будут приниматься пакеты, GIADDR которых равен 0 (данный Relay Agent является первой ретрансляцией данного пакета DHCP-

запроса), но у которых присутствует Relay Agent Information Option (Option 82). Если интерфейс не является доверенным, пакеты будут отброшены.

Если применены настройки команды `trust-all`, информация IP DHCP Relay является доверенной со всех интерфейсов. Если настройки данной команды не применены, статус информации определяется командой `ip dhcp relay information trusted` в режиме интерфейса.

Проверить настройки можно при помощи команды `show ip dhcp relay information trusted-sources`.

Пример

В данном примере показано, как на DHCP Relay Agent снять статус Trust для всех интерфейсов и запустить статус Trust для VLAN 100.

```
Switch# configure terminal
Switch(config)# no ip dhcp relay information trust-all
Switch(config)# interface vlan 100
Switch(config-if)# ip dhcp relay information trusted
Switch(config-if)#
```

19-14 ip dhcp local-relay vlan

Данная команда используется для включения Local Relay на одной из VLAN или группе VLAN. Используйте форму `no`, чтобы отключить данную функцию.

```
ip dhcp local-relay vlan VLAN-ID [, | -]
no ip dhcp local-relay vlan VLAN-ID [, | -]
```

Параметры

VLAN-ID	Укажите используемую VLAN.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Local Relay обеспечивает передачу сообщения DHCP на все локальные порты-участники VLAN на основе настроек Relay Option. Local Relay не изменяет IP-адрес и MAC-адрес назначения, а также поле шлюза пакета.



Примечание: если на интерфейсе отключена команда **ip dhcp relay**, интерфейс не будет ретранслировать или локально ретранслировать получаемые DHCP-пакеты.

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)#
```

19-15 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Наряду с пакетами DHCP Relay, подчиняющимися команде **ip helper-address**, Relay Destination DHCP-сервера можно указать в пуле DHCP Relay. Для этого войдите в режим настройки пула 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)#
```

19-16 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Наряду с пакетами DHCP Relay, подчиняющимся 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 наинтерфейсе, 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)#
```

19-17 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

<i>IP-ADDRESS</i>	Укажите IP-адрес сервера Relay Target для класса.
-------------------	---

По умолчанию

Нет

Режим ввода команды

DHCP Pool Class Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

В пуле DHCP Relay администратор может далее использовать команды **class** и **relay target**, чтобы связать список адресов Relay Target с классом DHCP. Если запрос клиента соответствует Relay-пулу, а пул DHCP Relay настроен с классами, для ретрансляции запрос клиента должен соответствовать классу, указанному в пуле. Если пакет не соответствует ни одному из классов пула, он не будет повторно ретранслирован. Если класс соответствующего Relay-пула не определен, запрос будет ретранслирован в Relay Destination

соответствующего Relay-пула. Для класса можно указать несколько команд Relay Target. Если пакет соответствует классу, он будет направлен во все Relay Targets (Destination).

Если для класса не настроена команда **relay target**, за Relay Target будет принято Relay Destination, указанное для пула. DHCP-пакет не будет ретранслирован, если на интерфейсе, принимающем пакет, не настроен IP-адрес.

Пример

В данном примере показано, как настроить DHCP Relay Target для ретрансляции пакетов, которая соответствует образцу значений опции, установленной в классе.

```
Switch# configure terminal
Switch(config)# ip dhcp class Service-A
Switch(config-dhcp-class)# option 60 hex 112233
Switch(config-dhcp-class)# option 60 hex 102030
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# relay source 172.19.18.0 255.255.255.0
Switch(config-dhcp-pool)# class Service-A
Switch(config-dhcp-pool-class)# relay target 10.2.1.2
Switch(config-dhcp-pool-class)#
```

19-18 show ip dhcp relay information trusted-sources

Данная команда используется для отображения всех интерфейсов, настроенных в качестве доверенных источников для опции DHCP Relay.

show ip dhcp relay information trusted-sources

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду для отображения рабочих настроек функции Trust Relay Option.

Пример

В данном примере показано, как отобразить список доверенных интерфейсов.

```
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 данном примере показано, как отображаются интерфейсы, если все они являются доверенными. Отдельные интерфейсы не отображаются.

```
Switch# show ip dhcp relay information trusted-sources

All interfaces are trusted source of relay agent information option

Switch#
```

19-19 show ip dhcp relay information option format-type

Данная команда используется для отображения настроек формата опций интерфейса.

show ip dhcp relay information option format-type [interface *INTERFACE-ID* [, | -]]

Параметры

<i>INTERFACE-ID</i>	(Опционально) Укажите для отображения информации об интерфейсе. Введите ID интерфейса после ключевого слова. Если ID интерфейса не указан, будет отображена информация обо всех интерфейсах.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения настроек формата опций интерфейса.

Пример

В данном примере показано, как отобразить настройки формата опций интерфейса.

```
Switch#show ip dhcp relay information option format-type

eth1/0/1
Remote ID vendor string: string1
eth1/0/2
Circuit ID vendor string: string1
eth1/0/3
Remote ID vendor string: string3
Circuit ID vendor string: string4

Total Entries: 3

Switch#
```

19-20 show ip dhcp relay information option-insert

Данная команда используется для отображения настройки встраивания Relay Option.

show ip dhcp relay information option-insert [interface *INTERFACE-ID* [, | -]]

Параметры

<i>INTERFACE-ID</i>	(Опционально) Укажите, чтобы отобразить информацию об интерфейсе. Введите ID интерфейса после ключевого слова. Если ID интерфейса не указан, будет отображена информация обо всех интерфейсах.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду для отображения Relay Information Option и информации о настройке встраивания.

Пример

В данном примере показано, как отобразить информацию об Option 82 и информацию о настройке встраивания этой опции для всех VLAN.

```
Switch# show ip dhcp relay information option-insert

Interface      Option-Insert
-----
vlan 1         Enabled
vlan 2         Disabled
vlan 3         Not Configured

Total Entries: 3

Switch#
```

19-21 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 [interface *INTERFACE-ID* [, | -]]

Параметры

<i>INTERFACE-ID</i>	(Опционально) Укажите, чтобы отобразить информацию об интерфейсе. Введите ID интерфейса после ключевого слова. Если ID интерфейса не указан, будет отображена информация обо всех интерфейсах.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду для отображения информации об алгоритме перенаправления Relay Option.

Пример

В данном примере показано, как отобразить информацию об алгоритме перенаправления Option 82 для всех VLAN.

```
Switch# show ip dhcp relay information policy-action

Interface      Policy
-----
vlan 1         Keep
vlan 2         Drop
vlan 3         Replace
vlan 4         Not configured

Total Entries: 3

Switch#
```

19-22 ip dhcp relay unicast

Данная команда позволяет настроить DHCP Relay и Local Relay Agent для обработки одноадресных DHCP-пакетов. Используйте форму **no**, чтобы отменить обработку одноадресных DHCP-пакетов.

```
ip dhcp relay unicast
no ip dhcp relay unicast
```

Параметры

Нет

По умолчанию

По умолчанию одноадресные пакеты DHCP-клиента будут ретранслированы.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для включения/отключения DHCP Relay и Local Relay Agent, чтобы запустить/отменить обработку одноадресных DHCP-пакетов.

Одноадресная передача включает в себя все типы сообщений DHCP-клиента, такие как DHCP Renew, DHCP Release и т. д. Если на нескольких устройствах в топологии запущен статус Relay, статус **unicast** должен быть идентичным. В ходе DHCP Relay не будет выявлено, какую именно роль выполняет VRRP при ретрансляции

пакета – Master или Slave. Пакеты всегда будут передаваться от первого Relay Agent, т. к. при обнаружении DHCP невозможно определить VRRP Master.

Пример

В данном примере показано, как запустить обработку одноадресных пакетов DHCP-клиента.

```
Switch# configure terminal
Switch(config)# ip dhcp relay unicast
Switch(config)#
```

19-23 ip dhcp relay information profile

Данная команда используется для того, чтобы задать профиль Option 82 и входа в режим Profile Configure Option 82. Используйте форму **no**, чтобы удалить указанный профиль Option 82.

```
ip dhcp relay information profile PROFILE-NAME
no ip dhcp relay information profile PROFILE-NAME
```

Параметры

<i>PROFILE-NAME</i>	Укажите имя профиля для определения профиля Option 82. Максимально допустимое количество символов – 32.
---------------------	--

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для входа в режим Profile Configure Option 82, чтобы задать профиль Option 82. При помощи профиля можно самостоятельно задать произвольную запись Option 82.

Пример

В данном примере показано, как войти в режим Profile Configure Option 82, чтобы задать профиль «remote_id».

```
Switch#configure terminal
Switch(config)#service dhcp
Switch(config)#ip dhcp relay information profile remote_id
Switch(config-dhcp-profile)#
```

19-24 format string

Данная команда используется для создания произвольной записи Option 82. Используйте форму **no**, чтобы удалить запись.

format string *FORMAT-STRING*
no format string

Параметры

FORMAT-STRING

Укажите формат Option 82 DHCP. Максимально допустимое количество символов – 255.

Ниже представлены правила конфигурирования данного параметра:

- Параметр может содержать шестнадцатеричные значения, строку ASCII или любую комбинацию шестнадцатеричных значений и строки ASCII. Строка ASCII должна быть заключена в кавычки (" "), например: "Ethernet". Символы ASCII вне кавычек будут распознаны как шестнадцатеричные значения.
- Отформатированная ключевая строка – строка, 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.

\$ 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 **ip dhcp 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для настройки записи Option 82, заданной пользователем.

Пример

В данном примере показано, как настроить запись Option 82, заданную пользователем.

```
switch#configure terminal
switch(config)# ip dhcp relay information profile profile1
switch(config-dhcp-profile)#format string Ethernet "%unit:"/0/ "%port:"\:%sysname:"%05svlan
switch(config-dhcp-profile)#
```

19-25 ip dhcp relay information option mac-format case

Данная команда используется для настройки формата MAC-адреса, задаваемого пользователем в профиле Option 82. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip dhcp relay information option mac-format case {lowercase | uppercase} delimiter {hyphen | colon |
dot | none } number {1 | 2 | 5}
no ip dhcp relay information option mac-format case
```

Параметры

lowercase	Укажите, чтобы использовать нижний регистр при записи MAC-адреса Option 82 для задаваемого пользователем профиля: aa-bb-cc-dd-ee-ff.
------------------	--

uppercase	Укажите, чтобы использовать верхний регистр при записи MAC-адреса Option 82 для задаваемого пользователем профиля: AA-BB-CC-DD-EE-FF.
hyphen	Укажите, чтобы использовать «-» в качестве разделителя данных: AA-BB-CC-DD-EE-FF.
colon	Укажите, чтобы использовать «:» в качестве разделителя данных: AA:BB:CC:DD:EE:FF.
dot	Укажите, чтобы использовать «.» в качестве разделителя данных: AA.BB.CC.DD.EE.FF.
none	Укажите для ввода данных без разделителя: AABBCCDDEEFF.
number	Укажите количество разделителей: 1: один разделитель: AABBCD.DDEEFF. 2: два разделителя: AABV.CCDD.EEFF. 5: несколько разделителей: AA.BB.CC.DD.EE.FF. Если указан параметр none, параметр number будет недействителен.

По умолчанию

Параметр регистра MAC-адреса аутентификации по умолчанию – **uppercase**.
Параметр разделителя MAC-адреса аутентификации по умолчанию – **none**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки формата MAC-адреса, заданного пользователем в профиле Option 82.

Пример

В данном примере показано, как настроить формат MAC-адреса, заданного пользователем в профиле Option 82.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information option mac-format case uppercase delimiter hyphen
number 5
Switch(config)#
```

19-26 show ip dhcp relay information profile

Данная команда используется для отображения настройки профиля Option 82 DHCP.

show ip dhcp relay information profile [NAME]

Параметры

<i>NAME</i>	(Опционально) Укажите, чтобы отобразить имя профиля Option 82.
-------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения настройки профиля Option 82 DHCP.

Пример

В данном примере показано, как отобразить настройки профиля Option 82 DHCP.

```
Switch# show ip dhcp relay information profile

Profile name: profile1
Format string: "Ethernet %unit:/0/ %port:\:%sysname:%05svlan"

Profile name: profile2
Format string: "Ethernet "%unit:"/0/ "%port:"\:%sysname:"%05svlan

Total Entries: 2

Switch#
```

19-27 show ip dhcp relay information option mac-format

Данная команда используется для отображения формата MAC-адреса в профиле Option 82.

show ip dhcp relay information option mac-format

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения формата MAC-адреса в профиле Option 82.

Пример

В данном примере показано, как отобразить формат MAC-адреса в профиле Option 82.

```
Switch#show ip dhcp relay information option mac-format
Case           : Uppercase
Delimiter      : Hyphen
Delimiter Number : 5
Example        : AA-BB-CC-DD-EE-FF
Switch#
```

19-28 ip dhcp relay

Данная команда используется для включения DHCP-Relay на интерфейсе. Используйте форму **no**, чтобы отключить данную функцию.

```
ip dhcp relay
no ip dhcp relay
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения/отключения DHCP Relay на физических портах или интерфейсах port-channel.

Пример

В данном примере показано, как включить обработку одноадресных пакетов DHCP-клиента на коммутаторе.

```
Switch#configure terminal
Switch(config)#service dhcp
Switch(config)#interface ethernet 1/0/2
Switch(config-if)#ip dhcp relay
Switch(config-if)#
```

20. Команды DHCP Server

20-1 address range

Данная команда используется для обозначения диапазона IP-адресов, которые необходимо ассоциировать с DHCP-классом в пуле DHCP-адресов. Используйте форму **no** для удаления диапазона адресов, которые необходимо ассоциировать с DHCP-классом.

```
address range START-IP-ADDRESS END-IP-ADDRESS
no address range START-IP-ADDRESS END-IP-ADDRESS
```

Параметры

<i>START-IP-ADDRESS</i>	Укажите адрес или первый адрес в диапазоне адресов.
<i>END-IP-ADDRESS</i>	Укажите последний адрес в диапазоне адресов.

По умолчанию

Нет

Режим ввода команды

DHCP Pool Class Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команды **address range** и **class** в конфигурации пула DHCP используются для того, чтобы ограничить выделение IP-адресов из подсети. Сеть разбивается на разделы на основе значения опции DHCP- запроса. Если в пуле адресов определены классы, то назначение адреса будет основано на классе этого адресного пула.

Когда сервер пытается выделить адрес из пула адресов, и если у пула определены классы, то сервер сначала проверит, содержит ли пул запрашиваемую подсеть. Если подсеть пула адресов содержит GIADDR (не равно нулю) или подсеть принимаемого интерфейса, то сервер будет выделять из пула адрес, соответствующий определенному классу.

Для удаления диапазона адресов можно указать только точный диапазон адресов, который уже был ранее настроен.

Пример

В данном примере показано, как создать DHCP-класс «Customer-A» с шаблоном, соответствующим Relay Information Option (Option 82). Он ассоциирован с диапазоном адресов DHCP «pool1».

```
Switch# configure terminal
Switch(config)# ip dhcp class Customer-A
Switch(config-dhcp-class)# option 82 hex 1234 *
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# network 172.28.5.0/24
Switch(config-dhcp-pool)# class Customer-A
Switch(config-dhcp-pool-class)# address range 172.28.5.1 172.28.5.12
Switch(config-dhcp-pool-class)#
```

20-2 bootfile

Используйте данную команду, чтобы указать файл конфигурации или файл образа для загрузки на устройство DHCP-клиента. Используйте форму **no**, чтобы удалить загрузочный файл.

bootfile *URL*
no bootfile

Параметры

<i>URL</i>	Укажите ссылку на файл загрузки. Максимально допустимая длина ссылки – 64 символа.
------------	--

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать файл конфигурации или файл образа для загрузки на устройство DHCP-клиента. Команда **next-server** указывает местоположение сервера, на котором находится загрузочный файл.

Пример

В данном примере показано, как указать файл «mdubootfile.bin» для DHCP-пула «pool1» в качестве загрузочного.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# bootfile \bootimage\mdubootfile.bin
Switch(config-dhcp-pool)#
```

20-3 clear ip dhcp binding

Данная команда используется для удаления записи привязки адресов из базы данных DHCP-сервера.

```
clear ip dhcp {all | pool NAME} binding {* | IP-ADDRESS}
```

Параметры

all	Укажите, чтобы очистить записи привязки всех пулов.
pool NAME	Укажите имя DHCP-пула.
*	Укажите, чтобы очистить все записи привязки, ассоциированные с указанным пулом.
IP-ADDRESS	Укажите IP-адрес записи привязки, которую необходимо удалить.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для удаления привязок адресов. Если задан параметр **pool**, а значение IP-адреса – *, то все автоматические записи привязок, ассоциированные с пулом, будут удалены. Если значение параметра **pool** – all, и IP-адрес указан, то автоматическая запись привязки, относящаяся к IP-адресу, будет удалена независимо от пула, в котором содержится запись привязки. Если указаны и параметр **pool**, и IP-адрес, автоматическая запись указанного IP-адреса в обозначенном пуле будет удалена.

Пример

В данном примере показано, как удалить привязку адреса 10.12.1.99 из базы данных DHCP-сервера.

```
Switch# clear ip dhcp all binding 10.12.1.99
Switch#
```

В данном примере показано, как удалить все привязки изо всех пулов.

```
Switch# clear ip dhcp all binding *
Switch#
```

В данном примере показано, как удалить привязку адреса 10.13.2.99 из пула адресов pool2.

```
Switch# clear ip dhcp pool pool2 binding 10.13.2.99
Switch#
```

20-4 clear ip dhcp conflict

Данная команда используется для удаления записи конфликта DHCP из базы данных DHCP-сервера.

clear ip dhcp {all | pool NAME} conflict {* | IP-ADDRESS}

Параметры

all	Укажите, чтобы удалить записи конфликтов для всех пулов.
pool NAME	Укажите имя DHCP-пула.
*	Укажите, чтобы удалить все записи конфликтов, ассоциированные с указанным пулом.
IP-ADDRESS	Укажите IP-адрес записи конфликта, которую необходимо.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для удаления адреса из таблицы конфликтов. Удаленный адрес будет возвращен в пул адресов и может быть использован в дальнейшем. DHCP-сервер обнаруживает конфликт IP-адреса при помощи операции Ping.

Если задан параметр **pool**, а значение IP-адреса – *, то все записи конфликта, относящиеся к пулу, будут удалены. Если значение параметра **pool** – all, и IP-адрес указан, то указанная запись конфликта будет удалена независимо от пула, в котором содержится запись конфликта. Если указаны и параметр **pool**, и IP-адрес, то обозначенная запись конфликта в соответствующем пуле будет удалена.

Пример

В данном примере показано, как удалить конфликт с адресом 10.12.1.99 из базы данных DHCP-сервера.

```
Switch# clear ip dhcp all conflict 10.12.1.99
Switch#
```

В данном примере показано, как удалить все адресные конфликты из базы данных DHCP-сервера.

```
Switch# clear ip dhcp all conflict *
Switch#
```

В данном примере показано, как удалить все адресные конфликты из пула адресов pool1.

```
Switch# clear ip dhcp pool pool1 conflict *
Switch#
```

В данном примере показано, как удалить конфликт с адресом 10.13.2.99 из пула адресов pool2.

```
Switch# clear ip dhcp pool pool2 conflict 10.13.2.99
Switch#
```

20-5 clear ip dhcp server statistics

Данная команда используется для сброса всех счетчиков DHCP-сервера.

clear ip dhcp server statistics

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для сброса всех счетчиков статистики DHCP.

Пример

В данном примере показано, как обнулить все счетчики DHCP.

```
Switch# clear ip dhcp server statistics
Switch#
```

20-6 class (DHCP Relay & Server)

Данная команда используется для входа в режим DHCP Pool Configuration Mode и привязки диапазона IP-адресов к DHCP-классу. Используйте форму **no** для удаления привязки.

class *NAME*
no class *NAME*

Параметры

<i>NAME</i>	Укажите имя DHCP-класса. Максимально допустимое количество символов – 32.
-------------	---

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команды **address range** и **class** в конфигурации пула DHCP используются для того, чтобы ограничить выделение IP-адресов из подсети. Сеть разбивается на разделы на основе значения опции DHCP-запроса.

Если в пуле адресов определены классы, то назначение адреса будет основано на классе этого адресного пула.

В пуле DHCP Relay пользователь может далее использовать команду **class** для привязки класса и DHCP-пула, а затем использовать Relay Targets, чтобы установить список адресов для передачи DHCP-пакетов. Если запрос клиента соответствует Relay-пулу, настроенному с классами, то для выполнения ретрансляции клиент должен соответствовать классу, настроенному в пуле. При отсутствии настроенных DHCP-классов запрос будет сопоставлен с Relay-пулом и будет ретранслирован на Relay Destination Server, указанный для соответствующего Relay-пула.

Пример

В данном примере показано, как создать два DHCP-класса Customer-A и Customer-B с соответствующими шаблонами Option 82. Они ассоциированы с диапазонами адресов DHCP-сервера «srv-pool1».

```
Switch# configure terminal
Switch(config)# ip dhcp class Customer-A
Switch(config-dhcp-class)# option 82 hex 1234 *
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp class Customer-B
Switch(config-dhcp-class)# option 82 hex 5678 *
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp pool srv-pool1
Switch(config-dhcp-pool)# network 172.28.5.0/24
Switch(config-dhcp-pool)# class Customer-A
Switch(config-dhcp-pool-class)# address-range 172.28.5.1 172.28.5.12
Switch(config-dhcp-pool-class)# exit
Switch(config-dhcp-pool)# class Customer-B
Switch(config-dhcp-pool-class)# address-range 172.28.5.18 172.28.5.32
Switch(config-dhcp-pool-class)#
```

В данном примере показано, как настроить DHCP-класс Service-A и задать соответствующий для него шаблон Option 60 DHCP 0x112233 и 0x102030. Другой класс Service-B настроен и задан с соответствующим ему шаблоном Option 60 DHCP 0x556677 и 0x506070. Класс Default-class настроен без опции. Эти заданные классы применяются в Relay-пуле «pool1». Класс Service-A ассоциирован с Relay Target 10.2.1.2, а класс Service-B ассоциирован с Relay Target 10.2.1.5. Класс Default-class ассоциирован с Relay Target 10.2.1.32.


```

Switch# configure terminal
Switch(config)# ip dhcp class Service-A
Switch(config-dhcp-class)# option 60 hex 112233
Switch(config-dhcp-class)# option 60 hex 102030
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp class Service-B
Switch(config-dhcp-class)# option 60 hex 556677
Switch(config-dhcp-class)# option 60 hex 506070
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp class Default-class
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# relay source 172.19.18 255.255.255.0
Switch(config-dhcp-pool)# class Service-A
Switch(config-dhcp-pool-class)# relay target 10.2.1.2
Switch(config-dhcp-pool-class)# exit
Switch(config-dhcp-pool)# class Service-B
Switch(config-dhcp-pool-class)# relay target 10.2.1.5
Switch(config-dhcp-pool-class)# exit
Switch(config-dhcp-pool)# class Default-class
Switch(config-dhcp-pool-class)# relay target 10.2.1.32
Switch(config-dhcp-pool)#

```

20-7 client-identifier

Данная команда используется для указания уникального ID DHCP-клиента в записи ручной привязки пула DHCP-адресов. Используйте форму **no** для удаления идентификатора клиента.

client-identifier *IDENTIFIER*
no client-identifier

Параметры

<i>IDENTIFIER</i>	Укажите идентификатор DHCP-клиента в шестнадцатеричном виде.
-------------------	--

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда действительна для записей привязок, созданных вручную в пуле DHCP. Идентификатор клиента формируется по типу среды передачи и MAC-адреса. В пуле DHCP-адресов может быть указана

только одна запись привязки, созданная вручную. При вводе записи привязки IP-адрес может быть связан с ID клиента или с аппаратным адресом узла.

Используйте команды **client-identifier** и **host**, чтобы указать запись привязки, созданной вручную на основе идентификатора клиента в DHCP-пакете.

Пример

В данном примере показано, как создать пул DHCP-адресов «pool1» с записью привязки, созданной вручную, которая связывает IP-адрес 10.1.2.3/24 с ID клиента 0x01524153203124.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# client-identifier 01524153203124
Switch(config-dhcp-pool)# host 10.1.2.3/24
Switch(config-dhcp-pool)#
```

20-8 default-router

Данная команда используется для указания шлюзов по умолчанию для DHCP-клиента. Используйте форму **no** для удаления шлюза по умолчанию.

default-router *IP-ADDRESS* [*IP-ADDRESS2...IP-ADDRESS8*]
no default-router *IP-ADDRESS* [*IP-ADDRESS2...IP-ADDRESS8*]

Параметры

<i>IP-ADDRESS</i>	Укажите IP-адрес шлюза по умолчанию для DHCP-клиента.
<i>IP-ADDRESS2...IP-ADDRESS8</i>	Укажите несколько IP-адресов, разделяя их при помощи пробелов. Максимально допустимое количество адресов – 8.

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки шлюза по умолчанию для клиента. IP-адрес шлюза должен принадлежать той же сети, что и подсеть клиента. Шлюзы перечислены в порядке приоритетности. Если шлюзы по умолчанию уже настроены, то шлюзы, настраиваемые позже, будут добавлены в список шлюзов по умолчанию.

Пример

В данном примере показано, как указать IP-адрес шлюза по умолчанию в пуле DHCP-адресов. Указанный IP-адрес – 10.1.1.1.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# default-router 10.1.1.1
```

20-9 domain-name

Данная команда используется для указания доменного имени для DHCP-клиента. Используйте форму **no** для удаления доменного имени.

domain-name *NAME*
no domain-name

Параметры

<i>NAME</i>	Укажите доменное имя. Максимально допустимое количество символов – 64.
-------------	--

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки доменного имени для DHCP-клиента. Можно указать не более одного доменного имени.

Пример

В данном примере показано, как указать доменное имя в пуле DHCP-адресов. Указанное доменное имя – «domain.com».

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# domain-name domain.com
```

20-10 dns-server

Данная команда используется для указания DNS-серверов для DHCP-клиента. Используйте форму **no** для удаления указанного DNS-сервера.

dns-server *IP-ADDRESS* [*IP-ADDRESS2*...*IP-ADDRESS8*]
no dns-server *IP-ADDRESS* [*IP-ADDRESS2*...*IP-ADDRESS8*]

Параметры

<i>IP-ADDRESS</i>	Укажите IP-адреса, которые будут использованы DHCP-клиентом в качестве DNS-сервера.
<i>IP-ADDRESS2...IP-ADDRESS8</i>	Укажите несколько IP-адресов, разделяя их при помощи пробелов. Максимально допустимое количество серверов – 8.

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки IP-адреса, который будет использован клиентом в качестве DNS-сервера. Максимально допустимое количество серверов – 8. Серверы перечисляются в порядке приоритетности. Если DNS-серверы уже настроены, то серверы, настраиваемые позже, будут добавлены в список DNS-серверов.

Пример

В данном примере показано, как указать IP-адрес DNS-сервера в пуле DHCP-адресов. Указанный IP-адрес – 10.1.1.1.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# default-router 10.1.1.1
```

20-11 hardware-address

Данная команда используется для указания аппаратного адреса в созданной вручную записи привязки пула DHCP-адресов. Используйте форму **no** для удаления аппаратного адреса созданной вручную записи привязки.

```
hardware-address HARDWARE-ADDRESS
no hardware-address
```

Параметры

<i>HARDWARE-ADDRESS</i>	Укажите MAC-адрес клиента.
-------------------------	----------------------------

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Запись привязки — это сопоставление IP-адреса с аппаратным адресом оборудования или ID клиента. При создании записи привязки IP-адрес присваивается клиенту вручную.

В пуле DHCP-адресов может быть указано не более одной записи привязки. С помощью записи привязки IP-адрес может быть связан с идентификатором клиента или с аппаратным адресом узла.

Используйте команды **client-identifier** и **host**, чтобы настроить ручную запись привязки на основе идентификатора клиента в DHCP-пакете. Команды **hardware-address** и **host** используются для настройки ручной записи привязки на основе аппаратного адреса.

Пример

В данном примере показано, как создать пул DHCP-адресов с настроенной вручную записью привязки, которая связывает IP-адрес 10.1.2.100/24 с MAC-адресом C2:F3:22:0A:12:F4. Указанное имя пула – «pool1».

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# hardware-address C2F3.220A.12F4
Switch(config-dhcp-pool)# host 10.1.2.100/24
Switch(config-dhcp-pool)#
```

20-12 host

Данная команда используется для указания IP-адреса в настроенной вручную записи привязки пула DHCP-адресов. Используйте форму **no** для удаления IP-адреса из записи.

```
host {IP-ADDRESS MASK | IP-ADDRESS/PREFIX-LENGTH}
no host
```

Параметры

<i>IP-ADDRESS</i>	Укажите IP-адрес в настроенной вручную записи привязки.
<i>MASK</i>	Укажите биты, определяющие сетевую маску.
<i>PREFIX-LENGTH</i>	Укажите длину префикса сети. Это альтернативный способ указать сетевую маску.

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

В пуле DHCP-адресов может быть указано не более одной записи привязки. С помощью записи привязки IP-адрес может быть связан с идентификатором клиента или с аппаратным адресом узла.

Используйте команды **client-identifier** и **host** для настройки вручную записи привязки на основе идентификатора клиента. Команды **hardware-address** и **host** используются для настройки вручную записи привязки на основе аппаратного адреса.

Пример

В данном примере показано, как создать пул DHCP-адресов с настроенной вручную записью привязки, которая связывает IP-адрес 10.1.2.100/24 с MAC-адресом C2:F3:22:0A:12:F4. Указанное имя пула – «pool1».

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# hardware-address C2:F3:22:0A:12:F4
Switch(config-dhcp-pool)# host 10.1.2.100/24
Switch(config-dhcp-pool)#
```

20-13 ip dhcp class (DHCP Relay & Server)

Данная команда используется для настройки DHCP-класса и входа в режим конфигурации DHCP-класса. Используйте форму **no** для удаления DHCP-класса.

```
ip dhcp class NAME
no ip dhcp class NAME
```

Параметры

<i>NAME</i>	Укажите имя DHCP-класса. Максимально допустимое количество символов – 32.
-------------	---

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для входа в режим конфигурации DHCP-класса. Затем при помощи команды **option hex** настройте соответствие шаблона опции с DHCP-классом. Если у класса отсутствует связь с шестнадцатеричной опцией, то классу будет соответствовать любой пакет.

Пример

В данном примере показано, как настроить DHCP-класс Service-A с соответствием шаблону 0x112233 Option 60 DHCP.

```
Switch# configure terminal
Switch(config)# ip dhcp class Service-A
Switch(config-dhcp-class)# option 60 hex 112233
Switch(config-dhcp-class)#
```

20-14 ip dhcp excluded-address

Данная команда используется для того, чтобы исключить диапазон IP-адресов для назначения клиенту. Используйте форму **no** для удаления исключенных адресов.

```
ip dhcp excluded-address START-IP-ADDRESS END-IP-ADDRESS
no ip dhcp excluded-address START-IP-ADDRESS END-IP-ADDRESS
```

Параметры

<i>START-IP-ADDRESS</i>	Укажите адрес или первый адрес диапазона адресов, которые необходимо исключить.
<i>END-IP-ADDRESS</i>	Укажите последний адрес диапазона адресов, которые необходимо исключить.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

DHCP-сервер автоматически распределяет адреса из пула DHCP-адресов по DHCP-клиентам. Для распределения доступны все адреса, кроме IP-адреса интерфейса шлюза и исключенных адресов, которые обозначены при помощи команды **ip dhcp excluded-address**. Можно отменить распределение нескольких диапазонов адресов. Для удаления диапазона исключенных адресов администратору необходимо указать точный диапазон данных адресов.

Пример

В данном примере показано, как исключить диапазон адресов. Указанный диапазон адресов: с 10.1.1.1 по 10.1.1.255 и с 10.2.1.1 по 10.2.1.255.

```
Switch# configure terminal
Switch(config)# ip dhcp excluded-address 10.1.1.1 10.1.1.255
Switch(config)# ip dhcp excluded-address 10.2.1.1 10.2.1.255
```

20-15 ip dhcp ping packets

Данная команда используется для указания количества пакетов, которое будет посылать DHCP-сервер в рамках Ping-операции. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ip dhcp ping packets *COUNT*
no ip dhcp ping packets

Параметры

<i>COUNT</i>	Укажите количество Ping-пакетов, которые будут отправлены DHCP-сервером.
--------------	--

По умолчанию

Значение по умолчанию – 2.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для указания количества пакетов, отправляемых DHCP-сервером в рамках Ping-операции. Ping-операция, выполняемая DHCP-сервером, позволяет определить наличие конфликта IP-адреса перед тем, как IP-адрес будет присвоен клиенту. При отсутствии ответа по истечении определенного количества попыток IP-адрес будет присвоен клиенту и занесен в запись. При получении сервером ответа на Ping-операцию IP-адрес будет занесен в запись конфликта.

Задайте 0, чтобы отключить Ping-операцию.

Пример

В данном примере показано, как указать количество Ping-пакетов. Указанное количество – 3.

```
Switch# configure terminal
Switch(config)# ip dhcp ping packets 3
Switch(config)#
```

20-16 ip dhcp ping timeout

Данная команда используется для указания времени ожидания ответного Ping-пакета DHCP-сервером. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip dhcp ping timeout MILLI-SECONDS
no ip dhcp ping timeout
```

Параметры

<i>MILLI-SECONDS</i>	Укажите период ожидания ответного Ping-пакета DHCP-сервером. Максимальный период ожидания – 10000 миллисекунд (10 секунд). Указанное значение должно быть кратным 100.
----------------------	--

По умолчанию

Значение по умолчанию – 500 миллисекунд (0,5 секунды).

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки периода ожидания Ping-операции. DHCP-сервер посылает Ping IP-адресу, чтобы определить, есть ли конфликт при использовании этого IP-адреса, прежде чем назначить IP-адрес клиенту. При отсутствии ответа по истечении определенного количества попыток IP-адрес будет присвоен клиенту и занесен в запись. При получении сервером ответа на Ping-операцию IP-адрес будет занесен в запись конфликта.

Пример

В данном примере показано, как настроить период ожидания ответа на Ping.

```
Switch# configure terminal
Switch(config)# ip dhcp ping timeout 800
Switch(config)#
```

20-17 ip dhcp pool (DHCP Server)

Данная команда используется для настройки пула DHCP-адресов DHCP-сервера и входа в режим настройки DHCP Pool Configuration Mode. Используйте форму **no** для удаления пула DHCP-адресов.

```
ip dhcp pool NAME
no ip dhcp pool NAME
```

Параметры

<i>NAME</i>	Укажите имя пула. Максимально допустимое количество символов – 32.
-------------	--

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Получив запрос от DHCP-клиента, DHCP-сервер выбирает IP-адрес из пула адресов и сообщает его клиенту. Пул адресов может содержать сеть IP-адресов или один IP-адрес. Используйте команду **network** в режиме DHCP Pool Configuration Mode, чтобы указать сеть для пула адресов. Команды **client-identifier**, **hardware-address** и **host** используются для настройки записи привязки вручную в пуле DHCP-адресов.

Пример

В данном примере показано, как создать пул DHCP-адресов. Указанное имя пула – «pool1».

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)#
```

20-18 ip dhcp use class

Данная команда используется для того, чтобы позволить DHCP-серверу использовать DHCP-классы при распределении адресов. Используйте форму **no**, чтобы отключить использование DHCP-классов.

```
ip dhcp use class
no ip dhcp use class
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для того, чтобы позволить DHCP-серверу использовать DHCP-классы при распределении адресов. Используйте форму **no**, чтобы отключить использование DHCP-классов.

Пример

В данном примере показано, как отключить использование DHCP-классов.

```
Switch# configure terminal
Switch(config)# no ip dhcp use class
Switch(config)#
```

20-19 lease

Данная команда используется для настройки периода аренды IP-адреса, назначаемого из пула адресов. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
lease {DAYS [HOURS [MINUTES]] | infinite}
no lease
```

Параметры

<i>DAYS</i>	Укажите период аренды в днях.
<i>HOURS</i>	(Опционально) Укажите период аренды в часах.
<i>MINUTES</i>	(Опционально) Укажите период аренды в минутах.
infinite	Период аренды не ограничен.

По умолчанию

Период аренды по умолчанию – 1 день.

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки периода аренды IP-адреса, присвоенного из пула адресов. Настройки родительского пула адресов не переходят на распределяемые IP-адреса автоматически.

Пример

В данном примере показано, как установить период аренды для пула адресов на 1 день. Указанное имя пула – «pool1».

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# lease 1
```

В данном примере показано, как установить период аренды для пула адресов на 1 час. Указанное имя пула – «pool1».

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# lease 0 1
```

20-20 netbios-node-type

Данная команда используется для настройки типа узла NetBIOS для DHCP-клиентов Microsoft. Используйте форму **no**, чтобы удалить настройки типа NetBIOS.

netbios-node-type *NTYPE*
no netbios-node-type

Параметры

<i>NTYPE</i>	Укажите тип узла NetBIOS для клиента Microsoft. Возможные типы узлов приведены ниже: b-node – Broadcast p-node – Peer-to-peer m-node – Mixed h-node – Hybrid
--------------	--

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки типа узла NetBIOS для DHCP-клиентов Microsoft. Рекомендуемый тип узла – H-Node (Hybrid). Тип узла определяет метод регистрации и разрешения имен, применяющийся в NetBIOS. В broadcast-системе используется тип broadcast. В системе P-Node применяются только запросы Point-to-Point на сервер имен (WINS). Система M-Node сначала начинает широковещательную рассылку, затем отправляет запрос на сервер имен. Hybrid-система сначала отправляет запрос на сервер имен, затем начинает широковещательную рассылку.

Пример

В данном примере показано, как настроить тип узла NetBIOS. Настроенный тип узла – H-Node.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# netbios-node-type h-node
Switch(config-dhcp-pool)#
```

20-21 netbios-name-server

Данная команда используется для указания WINS-серверов имен для DHCP-клиента Microsoft. Используйте форму **no** для удаления настроек указанных WINS-серверов.

netbios-name-server *IP-ADDRESS* [*IP-ADDRESS2...IP-ADDRESS8*]
no netbios-name-server *IP-ADDRESS* [*IP-ADDRESS2...IP-ADDRESS8*]

Параметры

<i>IP-ADDRESS</i>	Укажите IP-адрес WINS-сервера имен для DHCP-клиента.
<i>IP-ADDRESS2...IP-ADDRESS8</i>	Укажите несколько IP-адресов, разделяя их пробелами. Максимально допустимое количество серверов – 8.

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки IP-адресов WINS-сервера имен, доступных клиенту Microsoft. Максимально допустимое количество серверов – 8. Серверы указываются в порядке приоритетности. Если серверы имен уже настроены, то серверы, настраиваемые позже, будут добавлены в список серверов.

Пример

В данном примере показано, как настроить WINS-серверы 10.1.1.100 и 10.1.1.200 для пула адресов «pool1».

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# netbios-name-server 10.1.1.100 10.1.1.200
Switch(config-dhcp-pool)#
```

20-22 next-server

Данная команда используется для указания BOOT-сервера для DHCP-клиента. Используйте форму **no** для удаления Boot-серверов.

next-server *IP-ADDRESS*
no next-server

Параметры

<i>IP-ADDRESS</i>	Укажите IP-адрес Boot-сервера, чтобы обеспечить получение клиентом файла загрузки.
-------------------	--

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для указания IP-адреса сервера, чтобы обеспечить загрузку файла образа клиентом. Обычно используется TFTP-сервер. Максимально допустимое количество Boot-серверов – 1.

Пример

В данном примере показано, как настроить IP-адрес Next-Server в процессе загрузки DHCP-клиента в пуле pool1. Настроенный IP-адрес – 10.1.1.1.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# next-server 10.1.1.1
```

20-23 network

Данная команда используется для того, чтобы настроить подсеть для пула DHCP-адресов. Используйте форму **no** для удаления подсети.

```
network {NETWORK-ADDRESS MASK | NETWORK-ADDRESS/PREFIX-LENGTH}
no network
```

Параметры

<i>NETWORK-ADDRESS</i>	Укажите адрес подсети для пула адресов.
<i>MASK</i>	Укажите биты, определяющие сетевую маску.
<i>PREFIX-LENGTH</i>	Укажите длину префикса сети (это альтернативный способ указать сетевую маску).

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется в режиме DHCP Pool Configuration Mode, чтобы настроить подсеть для пула адресов. Невозможно сконфигурировать запись привязки вручную для того пула адресов, в котором указана подсеть.

Получая запрос от клиента, DHCP-сервер выбирает пул адресов или подсеть в пуле адресов на основе нижеуказанных правил распределения адресов. После присвоения узлу IP-адреса создается запись привязки.

- Если клиент не подключен к DHCP-серверу напрямую, сообщение Discover передается при помощи Relay Agent. Сервер выберет пул адресов с настроенной подсетью, содержащей GIADDR пакета, а затем присвоит адрес.
- Если клиент подключен к серверу напрямую, то сервер будет искать пулы, на которых настроена подсеть, которая соответствует подсети принимающего интерфейса.

Если адрес присвоен из указанной подсети, то сетевая маска, связанная с подсетью, будет использована в качестве сетевой маски пользователя. В качестве сети, настраиваемой для пула DHCP-адресов, может выступать сеть или подсеть. Настраиваемый пул DHCP-адресов организован в виде дерева: пул адресов, содержащий сеть, можно сравнить с корнем, пулы адресов, содержащие подсети – с ветвями, а пулы адресов, содержащие записи привязки вручную – с листьями. Дочерний пул адресов будет использовать все настройки родительского пула, кроме настроек аренды.

Пример

В данном примере показано, как настроить подсеть 10.1.0.0/16 для пула DHCP-адресов pool1.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# network 10.1.0.0/16
Switch(config-dhcp-pool)# default-router 10.1.1.1
Switch(config-dhcp-pool)#
```

20-24 option

Данная команда используется для настройки опций DHCP-сервера. Используйте форму **no** для удаления опции.

option *CODE* {*ascii STRING* | *hex {HEX-STRING | none}* | **ip** *IP-ADDRESS* [*IP-ADDRESS2...IP-ADDRESS8*]}
no option *CODE*

Параметры

<i>CODE</i>	Укажите номер опции в десятичной системе.
ascii <i>STRING</i>	Укажите формат строки ASCII для DHCP-опции. Максимально допустимое количество байт – 255.

hex	Укажите шестнадцатеричный формат для DHCP-опции. Максимально допустимое количество символов – 254.
<i>HEX-STRING</i>	Укажите шестнадцатеричную строку для DHCP-опции.
none	Укажите шестнадцатеричную строку нулевой длины.
ip <i>IP-ADDRESS</i>	Укажите IP-адрес. Максимально допустимое количество IP адресов – 8.

По умолчанию

Нет

Режим ввода команды

DHCP Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки DHCP-опций в DHCP-пуле. Настроить DHCP-опции можно также при помощи других команд: например, команды **default-router** в режиме DHCP Pool Configuration Mode. DHCP-сервер будет вносить все настраиваемые DHCP-опции во все ответные пакеты. Все настроенные DHCP-опции будут внесены в DHCP-пакеты, которые сервер отправляет в ответ.

Длина настраиваемой шестнадцатеричной строки должна быть выражена при помощи четного числа (так, 001100 – пример верного варианта числа, а 11223 – пример неверного варианта числа). Для одной опции можно указать одну строку.

Общая длина DHCP-опций ограничена. Ограничение по длине может быть установлено клиентом или сервером, если клиент не установил данное ограничение. Если ограничение не установлено, максимальная длина по умолчанию – 312.

Ниже перечислены опции, которые можно настроить при помощи других команд режима DHCP Pool Configuration Mode, но нельзя настроить при помощи команды **option**.

- Option 1 (Subnet Mask, настраивается при помощи команды **network**).
- Option 3 (Router Option, настраивается при помощи команды **default router**).
- Option 6 (Domain Name Server, настраивается при помощи команды **dns-server**).
- Option 15 (Domain Name, настраивается при помощи команды **domain-name**).
- Option 44 (NetBIOS Name Server, настраивается при помощи команды **netbios-name-server**).
- Option 46 (NetBIOS Node Type, настраивается при помощи команды **netbios-node-type**).
- Option 51 (IP Address Lease Time, настраивается при помощи команды **lease**).
- Option 58 (Renewal (T1) Time Value, настраивается при помощи команды **lease**).
- Option 59 (Rebinding (T2) Time Value, настраивается при помощи команды **lease**).

Ниже перечислены опции, которые не могут быть настроены при помощи команды **option**:

- Option 12 (Host Name, опция по умолчанию).
- Option 50 (Requested Address, опция по умолчанию).
- Option 53 (DHCP Message Type, опция по умолчанию).
- Option 54 (Server Identifier, опция по умолчанию).
- Option 55 (Parameter Request List, опция по умолчанию).

- Option 61 (Client Identifier, опция по умолчанию).
- Option 82 (Relay Agent Information Option, опция по умолчанию).

Пример

В данном примере показано, как настроить Option 69 DHCP-сервера (опцию SMTP-сервера) в шестнадцатеричном формате. Указанная шестнадцатеричная строка – c0a800fe (192.168.0.254).

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# option 69 hex c0a800fe
```

В данном примере показано, как настроить Option 40 DHCP-сервера (имя NIS-домена клиента) в формате строки ASCII.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# option 40 ascii net.market
```

В данном примере показано, как настроить Option 72 DHCP-сервера (опцию WWW-сервера) в формате IP. Настроенные WWW-серверы – 172.19.10.1 и 172.19.10.100.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# option 72 ip 172.19.10.1 172.19.10.100
```

20-25 option hex (DHCP Relay & Server)

Данная команда используется для настройки соответствия шаблона опции DHCP с классом DHCP. Используйте форму **no** для удаления соответствия.

option *CODE* hex *PATTERN* [*] [*bitmask* *MASK*]
no option *CODE* hex *PATTERN* [*] [*bitmask* *MASK*]

Параметры

<i>CODE</i>	Укажите номер DHCP-опции.
<i>PATTERN</i>	Укажите шестнадцатеричный шаблон указанной DHCP-опции.
*	Укажите биты опции, которые не будут проверяться на соответствие. При отсутствии отметки со знаком * длина шаблона опции должна быть равна битовой длине опции.
<i>MASK</i>	Укажите шестнадцатеричную битовую маску для шаблона. Указанные биты в маске будут проверены. Если маска не указана, будут проверены все биты, указанные в шаблоне. Будет проверен бит со значением 1. Формат ввода должен быть идентичен шаблону.

По умолчанию

Нет

Режим ввода команды

DHCP Class Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда **ip dhcp class**, наряду с командой **option hex**, может применяться для определения DHCP-класса. Классы в пуле распределяются в том порядке, в котором они настроены в пуле адресов.

Команда **option hex** применяется для указания номера DHCP-опции и сопоставления ему DHCP-класса. Для одного DHCP-класса можно указать несколько шаблонов опции. Если пакет соответствует какому-либо из указанных шаблонов, он будет причислен к DHCP-классу и передан указанное место назначения.

Ниже перечислены некоторые часто используемые коды опций:

- Option 60 (Vendor Class Identifier).
- Option 61 (Client Identifier).
- Option 77 (User Class).
- Option 82 (Relay Agent Information Option).
- Option 124 (Vendor-Identifying Vendor Class).
- Option 125 (Vendor-Identifying Vendor-Specific Information).

Пример

В данном примере показано, как настроить DHCP-класс Service-A и установить соответствие с ним шаблонов 0x112233 и 0x102030 Option 60 DHCP. Другой класс Service-B соответствует шаблонам 0x5566* и 0x5060* Option 60 DHCP.

```
Switch# configure terminal
Switch(config)# ip dhcp class Service-A
Switch(config-dhcp-class)# option 60 hex 112233
Switch(config-dhcp-class)# option 60 hex 102030
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp class Service-B
Switch(config-dhcp-class)# option 60 hex 5566 *
Switch(config-dhcp-class)# option 60 hex 5060 *
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp class Service-B
Switch(config-dhcp-class)#
```

20-26 service dhcp

Данная команда используется для включения DHCP-сервера и Relay Service. Для отключения данной команды используйте форму **no**.

```
service dhcp
no service dhcp
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для включения DHCP-сервера и Relay Service.

Пример

В данном примере показано, как отключить DHCP-сервер и Relay Service.

```
Switch# configure terminal
Switch(config)# no service dhcp
Switch(config)#
```

20-27 show ip dhcp binding

Данная команда используется для отображения записей привязки адресов DHCP-сервера.

show ip dhcp binding [IP-ADDRESS]

Параметры

<i>IP-ADDRESS</i>	(Опционально) Укажите, чтобы отобразить запись привязки. Если IP-адрес не указан, отображаются все записи привязки или записи привязки указанного пула.
-------------------	---

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Будет отображен IP-адрес, аппаратный адрес, сроки начала и истечения периода аренды записи.

Пример

В данном примере показано, как отобразить статус привязки всех связанных IP-адресов.

```
Switch#show ip dhcp binding

IP address      Client-ID/      Lease expiration  Type
                Hardware address
-----
10.0.0.1        01002211223344  Feb 25 2017 08:18 AM Automatic
Switch#
```

В данном примере показано, как отобразить статус привязки IP-адреса 10.1.1.1 в пуле DHCP адресов.

```
Switch#show ip dhcp binding

IP address      Client-ID/      Lease expiration  Type
                Hardware address
-----
10.1.1.1        01002211223344  Feb 25 2017 08:21 AM Automatic
Switch#
```

20-28 show ip dhcp conflict

Данная команда используется для отображения адресных конфликтов при попытках DHCP-сервера присвоить IP-адрес клиенту.

show ip dhcp conflict [IP-ADDRESS]

Параметры

<i>IP-ADDRESS</i>	(Опционально) Укажите, чтобы отобразить запись конфликта. Если IP-адрес не указан, отображаются все записи конфликта или записи конфликта указанного пула.
-------------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

DHCP-сервер обнаруживает конфликт IP-адресов при помощи Ping-операции. При обнаружении адресного конфликта данный IP-адрес будет удален из пула адресов и отмечен в качестве конфликтного. Этот адрес не может быть присвоен клиенту, пока администратор не устранит адресный конфликт.

Пример

В данном примере показано, как отобразить конфликтный статус IP-адреса 10.1.1.1.

```
Switch# show ip dhcp conflict 10.1.1.1

IP address      Detected Method Detection time
-----
10.1.1.1       Ping           Oct 23 2013 09:12 AM

Switch#
```

В данном примере показано, как отобразить конфликтный статус всех IP-адресов DHCP-пула.

```
Switch# show ip dhcp conflict

IP address      Detected Method Detection time
-----
10.1.1.1       Ping           Oct 23 2013 09:12 AM

Switch#
```

20-29 show ip dhcp pool

Данная команда используется для отображения информации о DHCP-пуле.

show ip dhcp pool [NAME]

Параметры

<i>NAME</i>	(Опционально) Укажите, чтобы отобразить информацию о DHCP-пуле. Если значение не задано, будет отображена информация обо всех DHCP-пулах.
-------------	---

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы просмотреть параметры настроек пула. Если значение не задано, будут отображены параметры конфигурации всех пулов.

Пример

В данном примере показано, как отобразить информацию о настройках DHCP-пула «pool1».

```
Switch#show ip dhcp pool pool1

Pool name: pool1
Network: 10.0.0.0/8
Boot file:
Default router:
DNS server:
NetBIOS server:
Domain name:
Lease: 1 days 0 hours 0 minutes
NetBIOS node type:
Next server: 0.0.0.0
Remaining unallocated address number: 1023
Number of leased addresses: 1

Switch#
```

20-30 show ip dhcp server

Данная команда используется для отображения текущего статуса DHCP-сервера.

show ip dhcp server

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить статус DHCP-сервера и пул адресов, настроенный пользователем.

Пример

В данном примере показано, как отобразить статус DHCP-сервера.

```

Switch# show ip dhcp server

DHCP Service: Disable
Ping packets number: 3
Ping timeout: 500 ms
Excluded Addresses
10.1.1.1-10.1.1.255

List of DHCP server configured address pool
pool1          pool2          pool3          pool4
pool5          pool6          pool7          pool8
pool9          pool10         pool11         pool12

Switch#

```

20-31 show ip dhcp server statistics

Данная команда используется для отображения статистики DHCP-сервера.

show ip dhcp server statistics

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить счетчики DHCP. Все счетчики суммируются.

Пример

В данном примере показано, как отобразить статистику DHCP-сервера.

```
Switch# show ip dhcp server statistics
```

```
Address pools          3
Automatic bindings    100
Manual binding         2
Malformed messages    0
Renew messages        0
```

```
Message                Received
BOOTREQUEST            12
DHCPDISCOVER           200
DHCPRREQUEST          178
DHCPDECLINE            0
DHCPRELEASE            0
DHCPIFORM              0
```

```
Message                Sent
BOOTREPLY              12
DHCPOFFER              190
DHCPACK                172
DHCNPAK                6
```

```
Switch#
```

Отображаемые параметры

Address pools	Количество пулов, настроенных в базе данных DHCP.
Malformed messages	Количество поврежденных сообщений, полученных DHCP сервером.
Renew messages	Количество Renew-сообщений для времени аренды DHCP. Счетчик увеличивается, когда поступает новое Renew-сообщение о продлении аренды.
Message	Тип DHCP-сообщения.
Received	Количество DHCP-сообщений, полученных DHCP-сервером.
Sent	Количество DHCP-сообщений, отправленных DHCP-сервером.

21. Команды DHCP Server Screening

21-1 based-on hardware-address

Данная команда используется для добавления записи профиля DHCP Server Screen. Используйте форму **no** для удаления записи.

based-on hardware-address *CLIENT-HARDWARE-ADDRESS*
no based-on hardware-address *CLIENT-HARDWARE-ADDRESS*

Параметры

<i>CLIENT-HARDWARE-ADDRESS</i>	Укажите MAC-адрес клиента.
--------------------------------	----------------------------

По умолчанию

Нет

Режим ввода команды

Configure DHCP Server Screen Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Будет разрешена отправка сообщения сервера с IP-адресом указанного сервера и адресом клиента в пакете. Согласно данным записям привязок, только указанным серверам разрешено назначать адреса указанным клиентам.

Пример

В данном примере показано, как настроить профиль DHCP Server Screen «campus-profile», содержащий список MAC-адресов клиентов.

```
Switch# configure terminal
Switch(config)# dhcp-server-screen profile campus-profile
Switch(config-dhcp-server-screen)# based-on hardware-address 00-08-01-02-03-04
Switch(config-dhcp-server-screen)# based-on hardware-address 00-08-01-03-00-01
Switch(config-dhcp-server-screen)#
```

21-2 clear ip dhcp snooping server-screen log

Используйте данную команду, чтобы очистить буфер журнала событий Server Screen.

clear ip dhcp snooping server-screen log

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы очистить буфер журнала событий Server Screen. Буфер журнала событий DHCP Server Screen хранит информацию о пакетах, которые не прошли screening. Первый пакет, который не прошел проверку, будет отправлен в модуль журнала событий и записан в буфер журнала событий Server Screen. Последующие пакеты из той же сессии не будут отправлены в модуль журнала событий, если его запись в буфере журнала событий не будет удалена.

Пример

В данном примере показано, как очистить журнал событий Server Screen.

```
Switch# clear ip dhcp snooping server-screen log
Switch#
```

21-3 dhcp-server-screen profile

Данная команда используется для настройки профиля Server Screen и входа в режим Server ScreenConfigure Mode. Используйте форму **no** для удаления профиля Server Screen.

dhcp-server-screen profile *PROFILE-NAME*
no dhcp-server-screen profile *PROFILE-NAME*

Параметры

<i>PROFILE-NAME</i>	Укажите имя профиля. Максимально допустимое количество символов – 32.
---------------------	---

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы войти в режим DHCP Server Screen Configure Mode и настроить профиль Server Screen. Профиль можно использовать для настройки записи DHCP Server Screen.

Пример

В данном примере показано, как войти в режим DHCP Server Screen Configure Mode и настроить профиль «campus».

```
Switch# configure terminal
Switch(config)# service dhcp
Switch(config)# dhcp-server-screen profile campus
Switch(config-dhcp-server-screen)#
```

21-4 ip dhcp snooping server-screen

Данная команда используется для включения DHCP Server Screening. Используйте форму **no** для отключения данной функции.

ip dhcp snooping server-screen [*SERVER-IP-ADDRESS* **profile** *PROFILE-NAME*]
no ip dhcp snooping server-screen [*SERVER-IP-ADDRESS*]

Параметры

<i>SERVER-IP-ADDRESS</i>	(Опционально) Укажите IP-адрес доверенного DHCP-сервера.
profile <i>PROFILE-NAME</i>	(Опционально) Укажите профиль со списком MAC-адресов клиентов для DHCP-сервера.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для настройки физического порта и port-channel.

Функция DHCP Server Screening используется для фильтрации пакетов DHCP-сервера на указанном интерфейсе, а также для получения доверенных пакетов из указанного источника. Данная функция может сделать используемую сеть защищенной в случае, когда DHCP-Server пакеты отправляются вредоносным узлом.

Если IP-адрес сервера не указан, на интерфейсе будет включен/отключен DHCP Server Screen. По умолчанию DHCP Server Screen отключен на всех интерфейсах. Если DHCP Server Screen включен, все пакеты DHCP-сервера на указанном интерфейсе будут отфильтрованы и будут переданы только пакеты от доверенного сервера.

Если запись Server Screen определена в профиле, который содержит MAC-адрес клиента, будет передано сообщение сервера с IP-адресом сервера и адресами клиентов, содержащимися в профиле.

Если запись настроена без MAC-адреса клиента, будет передано сообщение сервера с IP-адресом указанного сервера. Каждый сервер может иметь только одну соответствующую запись в таблице.

Если запись определена в профиле, но записи не существует, сообщения с IP-адресом сервера, указанным в записи, не передаются.

Пример

В данном примере показано, как настроить профиль DHCP Server Screen «campus-profile» и ассоциировать его с записью DHCP Server Screen для Ethernet 1/0/3.

```
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 ethernet 1/0/3
Switch(config-if)# ip dhcp snooping server-screen 10.1.1.2 profile campus-profile
Switch(config-if)#
```

21-5 ip dhcp snooping server-screen log-buffer

Данная команда используется для настройки параметра буфера журнала событий DHCP ServerScreen. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ip dhcp snooping server-screen log-buffer entries *NUMBER*
no ip dhcp snooping server-screen log-buffer entries

Параметры

<i>NUMBER</i>	Укажите количество записей в буфере. Максимальное значение – 1024.
---------------	--

По умолчанию

Значение по умолчанию – 32.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки максимального количества записей в буфере журнала событий. Буфер журнала событий DHCP Server Screen хранит информацию о пакетах, которые не прошли screening. Первый пакет, который не прошел проверку, будет отправлен в модуль журнала событий и записан в буфер журнала событий Server Screen. Последующие пакеты из той же сессии не будут отправлены в модуль журнала событий, если его запись в буфере журнала не будет удалена.

Если буфер журнала событий полон, но события (нарушения) продолжают поступать, пакеты будут отброшены, а события не будут отправлены в модуль системного журнала. Если пользователь задает размер буфера меньше текущего номера записи, буфер журнала будет очищен автоматически.

Пример

В данном примере показано, как изменить размер буфера на 64.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping server-screen log-buffer entries 64
Switch(config)#
```

21-6 show ip dhcp server-screen log

Данная команда используется для отображения буфера журнала событий Server Screen.

show ip dhcp server-screen log

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить содержимое буфера журнала событий DHCP Server Screen. Буфер хранит информацию о сообщениях сервера, которые не прошли screening. Фиксируется количество нарушений одного и того же типа, а также время последнего нарушения.

Пример

В данном примере показано, как отобразить буфер журнала событий DHCP Server Screen.

```
Switch# show ip dhcp server-screen log

Total log buffer size: 64

VLAN          Server IP          Client MAC          Occurrence
-----
100           10.20.1.1          00-20-30-40-50-60  06:30:37, 2013-02-07
100           10.58.2.30         10-22-33-44-50-60  06:31:42, 2013-02-07

Total Entries: 2

Switch#
```

21-7 snmp-server enable traps dhcp-server-screen

Данная команда используется для включения отправки SNMP-уведомлений об атаках, поступающих от ложного DHCP-сервера. Используйте форму **no** для отключения отправки SNMP-уведомлений.

snmp-server enable traps dhcp-server-screen
no snmp-server enable traps dhcp-server-screen

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если после запуска функции DHCP Server Screening коммутатор получил от ложного DHCP-сервера атакующий пакет, данное событие будет занесено в журнал. Используйте данную команду, чтобы включить/отключить отправки SNMP-уведомлений о подобных событиях.

Пример

В данном примере показано, как включить отправки trap-сообщений для DHCP Server Screening.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps dhcp-server-screen
Switch(config)#
```

22. Команды DHCP Snooping

22-1 ip dhcp snooping

Данная команда используется для глобального включения DHCP Snooping. Используйте форму **no**, чтобы отключить DHCP Snooping.

```
ip dhcp snooping
no ip dhcp snooping
```

Параметры

Нет

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Функция DHCP Snooping отслеживает пакеты DHCP, поступающие на недоверенный интерфейс во VLAN, на котором включена данная функция. С помощью данной функции DHCP-пакеты, приходящие с недоверенного интерфейса, могут получить статус проверенных и будет создана таблица привязки DHCP для DHCP Snooping во VLAN. Таблица привязки содержит информацию о привязке IP и MAC, которая позже дополнительно может использоваться IP Source Guard и Dynamic ARP Inspection.

Пример

В данном примере показано, как включить DHCP Snooping.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping
Switch(config)#
```

22-2 ip dhcp snooping information option allow-untrusted

Данная команда используется для глобального доступа DHCP-пакетов с Relay Option 82 к недоверенным интерфейсам. Используйте форму **no**, чтобы запретить пакеты с Relay Option 82.

```
ip dhcp snooping information option allow-untrusted
no ip dhcp snooping information option allow-untrusted
```

Параметры

Нет

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Функция DHCP Snooping проверяет пакеты DHCP, когда они поступают на порт во VLAN, на котором включена функция DHCP Snooping. По умолчанию при проверке будут отброшены пакеты, если их адрес шлюза не равен 0 или присутствует Option 82.

Используйте данную команду, чтобы разрешить пакетам с Relay Option 82 доступ к недоверенным интерфейсам.

Пример

В данном примере показано, как включить DHCP Snooping для Option 82, чтобы разрешить доступ к недоверенным интерфейсам.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping information option allow-untrusted
Switch(config)#
```

22-3 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"> ftp://username:password@location:tcpport/filename tftp://location/filename flash://filename
write-delay SECONDS	Укажите время ожидания перед обновлением записи при обнаружении изменений в таблице привязки. Время по умолчанию составляет 300 секунд. Диапазон доступных значений от 60 до 86400.

По умолчанию

По умолчанию URL-адрес агента базы данных не установлен.
Значение времени задержки для записи по умолчанию составляет 300 секунд.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для хранения записей привязки DHCP в локальной Flash-памяти или на удаленном узле. Используйте следующие методы для хранения записей привязки DHCP:

- **flash:** хранение записей в файле в локальной файловой системе.
- **tftp:** хранение записей на удаленном узле через TFTP.
- **ftp:** хранение записей на удаленном узле через FTP.



Примечание: Flash-память включает в себя только внешнюю память, например, USB-флеш накопитель.

Используйте данную команду, чтобы сохранить таблицу привязки DHCP Snooping в коммутаторе стека. Таблица не будет сохранена в отдельных коммутаторах стека.

Время аренды записи (Lease Time) не будет изменено, и время жизни (Live Time) продолжит отсчитываться, пока запись существует.

Пример

В данном примере показано, как настроить сохранение привязки в файл файловой системы.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping database tftp: //10.0.0.2/store/dhcp-snp-bind
Switch(config)#
```

22-4 clear ip dhcp snooping database statistics

Данная команда используется для удаления статистики таблицы привязки DHCP.

clear ip dhcp snooping database statistics

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет удалить статистику таблицы привязки DHCP.

Пример

В данном примере показано, как удалить статистику таблицы привязки DHCP Snooping.

```
Switch# clear ip dhcp snooping database statistics
Switch#
```

22-5 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.
vlan <i>VLAN-ID</i>	(Опционально) Укажите VLAN ID, который необходимо удалить.
interface <i>INTERFACE-ID</i>	(Опционально) Укажите интерфейс, который необходимо удалить.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет удалить запись привязки DHCP, включая заданные вручную записи привязки.

Пример

В данном примере показано, как удалить все записи привязки DHCP Snooping.

```
Switch# clear ip dhcp snooping binding
Switch#
```

22-6 renew ip dhcp snooping database

Данная команда используется для обновления таблицы привязки DHCP.

renew ip dhcp snooping database URL

Параметры

<i>URL</i>	<p>Укажите URL места, из которых нужно загружать таблицу привязки для обновления.</p> <p>URL может быть в одном из следующих форматов:</p> <ul style="list-style-type: none"> • ftp://username:password@location:tcpport/filename • tftp://location/filename • flash:/filename
------------	---

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для обновления таблицы привязки DHCP с URL-адреса и добавления записей в таблицу привязки DHCP Snooping.

Используйте следующие методы для загрузки привязки DHCP Snooping:

- **flash:** загрузка записей из файла в локальной файловой системы.
- **tftp:** загрузка записей с удаленного узла через TFTP.
- **ftp:** загрузка записей с удаленного узла через FTP.



Примечание: Flash-память включает в себя только внешнюю память, например, USB-флеш накопитель.

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#
```

22-7 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-ID expiry
SECONDS
```

Параметры

<i>MAC-ADDRESS</i>	Укажите MAC-адрес записи, которую необходимо добавить или удалить.
<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.
interface <i>INTERFACE-ID</i>	Укажите интерфейс (физический порт или port-channel), на котором необходимо добавить или удалить запись привязки.
expiry <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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для создания динамической записи DHCP Snooping.

Пример

В данном примере показано, как настроить запись DHCP Snooping с IP-адресом 10.1.1.1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 и порту Ethernet 1/0/10 с expiry time 100 секунд.

```
Switch# ip dhcp snooping binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface ethernet 1/0/10
expiry 100
Switch#
```

22-8 ip dhcp snooping trust

Данная команда используется для настройки порта в качестве доверенного интерфейса для DHCP Snooping. При использовании формы **no** команда вернется к значениям по умолчанию.

```
ip dhcp snooping trust
no ip dhcp snooping trust
```

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет настроить физический порт и port-channel интерфейс.

Порты, подключенные к DHCP-серверу или к другим коммутаторам, должны быть настроены как доверенные интерфейсы. Порты, подключенные к DHCP-клиентам, должны быть настроены как недоверенные интерфейсы. DHCP Snooping работает в качестве межсетевого экрана между недоверенными интерфейсами и DHCP-серверами.

Если порт настроен как недоверенный интерфейс, сообщение DHCP придет на порт в ту VLAN, в которой включен DHCP Snooping. Коммутатор перенаправит пакеты DHCP, если только не будет соблюдаться любое из следующих условий (в таком случае пакеты будут отбрасываться):

- Порт коммутатора получает пакет (например, пакет DHCP OFFER, DHCP ACK, DHCP NAK или DHCP LEASE QUERY) 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 данном примере показано, как настроить DHCP Snooping для доверенного порта 1/0/3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)#
```

22-9 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-limit}
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.
no-limit	Укажите для снятия ограничения количества записей.

По умолчанию

По умолчанию ограничений на количество записей нет.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет настроить физический порт и интерфейс port-channel. Команда действует только на недоверенных интерфейсах. Система перестанет изучать привязки, связанные с портом, если превышено максимальное значение.

Пример

В данном примере показано, как настроить ограничение количества привязок (используется значение 100) для Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ip dhcp snooping limit entries 100
Switch(config-if)#
```

22-10 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-limit}
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.
--------------	---

no-limit

Укажите для снятия ограничения скорости.

По умолчанию

По умолчанию ограничений нет.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

При превышении лимита количества DHCP-пакетов за секунду порт будет отключен из-за ошибки.

Пример

В данном примере показано, как настроить количество сообщений DHCP, которое коммутатор сможет получить на порту 1/0/3 за одну секунду.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)#
```

22-11 ip dhcp snooping station-move deny

Данная команда используется для отключения состояния DHCP Snooping Station Move. При использовании формы **no** команда включит состояние DHCP Snooping Roaming.

```
ip dhcp snooping station-move deny
no ip dhcp snooping station-move deny
```

Параметры

Нет

По умолчанию

По умолчанию опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

При включении DHCP Snooping Station Move динамическая запись привязки DHCP Snooping с теми же VLAN ID и MAC-адресом на определенном порту может переместиться на другой порт, если обнаружится, что новому процессу DHCP принадлежит тот же VLAN ID и MAC-адрес.

Пример

В данном примере показано, как отключить состояние Roaming.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping station-move deny
Switch(config)#
```

22- 12 ip dhcp snooping verify mac-address

Данная команда используется для включения проверки совпадения MAC-адреса источника DHCP-пакета и аппаратного адреса клиента. При использовании формы **no** команда отключит проверку MAC-адреса.

ip dhcp snooping verify mac-address
no ip dhcp snooping verify mac-address

Параметры

Нет

По умолчанию

По умолчанию опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Функция DHCP Snooping проверяет DHCP пакеты, присылаемые на порт во VLAN, на которой включена функция DHCP Snooping. По умолчанию DHCP Snooping проверяет, совпадает ли MAC- адрес источника в заголовке Ethernet с аппаратным адресом DHCP-клиента, чтобы пройти проверку.

Пример

В данном примере показано, как включить проверку на соответствие MAC-адреса источника DHCP- пакета аппаратному адресу клиента.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping verify mac-address
Switch(config)#
```

22- 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>	Укажите VLAN, в которой необходимо включить или отключить функцию DHCP Snooping.
,	(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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для глобального включения DHCP Snooping, используйте команду **ip dhcp snooping vlan** для включения DHCP Snooping для VLAN. Функция DHCP Snooping отслеживает пакеты DHCP, приходящие на недоверенный интерфейс во VLAN, на которой включена функция DHCP snooping. С помощью данной функции DHCP-пакеты, приходящие с недоверенного интерфейса, могут получить статус проверенных, а таблица привязки DHCP будет создана для DHCP Snooping во VLAN. Таблица привязки предоставляет информацию о привязке IP и MAC, которая позже может использоваться IP Source Guard и Dynamic ARP Inspection.

Пример

В данном примере показано, как включить DHCP Snooping во VLAN 10.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping vlan 10
Switch(config)#
```

В данном примере показано, как включить DHCP Snooping в нескольких VLAN.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping vlan 10,15-18
Switch(config)#
```

22-14 show ip dhcp snooping

Данная команда используется для отображения настроек DHCP Snooping.

show ip dhcp snooping

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения параметров настроек DHCP Snooping.

Пример

В данном примере показано, как включить отображение параметров настроек DHCP Snooping.

```
Switch# show ip dhcp snooping

DHCP Snooping is enabled
DHCP Snooping is enabled on VLANs:
    10, 15-18
Verification of MAC address is disabled
Station move is permitted.
Information option is not allowed on un-trusted interface

Interface      Trusted  Rate Limit  Entry Limit
-----
eth1/0/1       no       10          no_limit
eth1/0/2       no       50          no_limit
eth1/0/3       yes      no_limit    no_limit

Switch#
```

22-15 show ip dhcp snooping binding

Данная команда используется для отображения привязки DHCP Snooping.

**show ip dhcp snooping binding [IP-ADDRESS] [MAC-ADDRESS] [vlan VLAN-ID] [interface INTERFACE-ID
[, | -]]**

Параметры

<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.
<i>VLAN-ID</i>	(Опционально) Укажите, если необходимо отображать привязки на основе VLAN.
<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

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения привязки DHCP Snooping.

Пример

В данном примере показано, как настроить отображение 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 10.1.1.1 00-01-02-03-04-05 vlan 100
```

MAC Address	IP Address	Lease (seconds)	Type	VLAN	Interface
00-01-02-03-04-05	10.1.1.1	1500	dhcp-snooping	100	eth1/0/5

Total Entries: 1

```
Switch#
```

В данном примере показано, как настроить отображение привязки DHCP Snooping во VLAN 100.

```
Switch# show ip dhcp snooping binding vlan 100
```

MAC Address	IP Address	Lease (seconds)	Type	VLAN	Interface
00-01-02-03-04-05	10.1.1.10	1500	dhcp-snooping	100	eth1/0/5
00-01-02-00-00-05	10.1.1.11	1495	dhcp-snooping	100	eth1/0/5

Total Entries: 2

```
Switch#
```

В данном примере показано, как настроить отображение привязки DHCP Snooping на интерфейсе Ethernet 1/0/5.

```
Switch# show ip dhcp snooping binding interface ethernet 1/0/5

MAC Address      IP Address      Lease (seconds) Type          VLAN Interface
-----
00-01-02-03-04-05 10.1.1.10      1500          dhcp-snooping 100 eth1/0/5
00-01-02-00-00-05 10.1.1.11      495           dhcp-snooping 100 eth1/0/5

Total Entries: 2

Switch#
```

Отображаемые параметры

MAC-адрес	Аппаратный MAC-адрес клиента.
IP-адрес	IP-адрес клиента, назначенный DHCP-сервером.
Время аренды (lease) (в секундах)	Время аренды IP-адреса.
Тип	Тип привязки, настроенный через интерфейс командной строки или изученный динамически.
VLAN	VLAN ID.
Interface	Интерфейс, подключающийся к узлу DHCP-клиента.

22-16 show ip dhcp snooping database

Данная команда используется для отображения статистики таблицы привязки DHCP Snooping.

show ip dhcp snooping database

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения статистики таблицы привязки DHCP Snooping.

Пример

В данном примере показано, как включить отображение статистики таблицы привязки DHCP Snooping.

```

Switch#show ip dhcp snooping database

URL: tftp: //10.0.0.2/store/dhcp-snp-bind
Write Delay Time: 300 seconds

Last ignored bindings counters:
Binding collisions : 0          Expired lease : 0
Invalid interfaces : 0          Unsupported vlans : 0
Parse failures    : 0          Checksum errors : 0

Switch#

```

Отображаемые параметры

Binding Collisions	Количество записей, создавших коллизии с существующими записями в таблице привязки DHCP Snooping.
Expired leases	Количество записей с истекшим сроком аренды в таблице привязки DHCP Snooping.
Invalid interfaces	Количество интерфейсов, получивших сообщение DHCP, но DHCP Snooping для которых не выполняется.
Pase failures	Количество недопустимых пакетов DHCP.
Checksum errors	Количество подсчитанных значений checksum, не равное сохраненному значению checksum.
Unsupported vlans	Количество записей, для которых VLAN отключена.

23. Команды DHCPv6 Client

23-1 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для перезапуска IPv6 DHCP Client на указанном интерфейсе.

Пример

В данном примере показано, как перезапустить DHCPv6 Client для интерфейса VLAN 1.

```
Switch# clear ipv6 dhcp client vlan 1
Switch#
```

23-2 ipv6 dhcp client pd

Используйте данную команду, чтобы включить запрос Dynamic Host Configuration Protocol (DHCP) IPv6 Client для делегирования префикса (Prefix Delegation) через указанный интерфейс. Используйте форму **no**, чтобы отключить запрос.

```
ipv6 dhcp client pd {PREFIX-NAME} [rapid-commit]
no ipv6 dhcp client pd
```

Параметры

<i>PREFIX-NAME</i>	Укажите имя основного префикса IPv6. Максимально допустимое количество символов – 12.
--------------------	--

rapid-commit	Укажите, чтобы получать сетевые настройки от DHCPv6-сервера по средством быстрого обмена двумя сообщениями вместо стандартных четырех между Requesting Router (RR) и Delegating Router (DR).
---------------------	--

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить запрос Prefix Delegation (PD) через интерфейс. На конфигурируемом интерфейсе будет включен режим DHCP Client Mode. Префикс, полученный от сервера, будет храниться в общем пуле префиксов IPv6, указанном в команде в качестве имени общего префикса, который будет использован в конфигурации IPv6-адресов.

Можно указать только одно имя основного префикса для DHCPv6 PD на интерфейсе. При этом одно и то же имя основного префикса можно указать для DHCPv6 PD на нескольких интерфейсах.

Стандартный обмен сообщениями между маршрутизаторами DR и RR включает в себя четыре типа сообщений: *SOLICIT*, *ADVERTISE*, *REQUEST* и *REPLY*. При использовании параметра **rapid-commit** маршрутизаторы обмениваются двумя сообщениями вместо четырех. В этом случае маршрутизатор RR отправит маршрутизатору DR сообщение *SOLICIT*, в котором уведомит его о возможности пропустить получение сообщения *ADVERTISE* и отправку сообщения *REQUEST* и перейти непосредственно к получению сообщения *REPLY* от маршрутизатора DR. В сообщении *REPLY* содержится информация по сетевым настройкам.

Для корректной работы данного функционала необходимо включить параметр **rapid-commit** и на DR, и на RR.

Если клиент получает advertisement от нескольких серверов, будет выбран сервер с наивысшим приоритетом. Клиент может принять несколько префиксов, делегированных сервером.

Для IPv6 Client функции DHCP Server DHCP Relay несовместимы на одном интерфейсе.

Пример

В данном примере показано, как сконфигурировать IPv6-адрес на VLAN 2 на основе общего префикса «dhcp-prefix» и включить делегирование префикса DHCPv6 (Prefix Delegation) на VLAN 1 с общим именем префикса «dhcp-prefix» и опцией Rapid Commit.


```
Switch# configure terminal
Switch(config)# interface vlan 2
Switch(config-if)# ipv6 address dhcp-prefix 0:0:0:7272::72/64
Switch(config-if)# exit
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 dhcp client pd dhcp-prefix rapid-commit
Switch(config-if)#
```

23-3 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

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить DHCPv6 DUID устройства, или используйте команду **show ipv6 dhcp interface**, чтобы отобразить настройки DHCPv6 для интерфейсов. Если ID интерфейса не указан, будут отображены все интерфейсы с функцией DHCPv6.

Пример

В данном примере показано, как отобразить DHCPv6 DUID для устройства.

```
Switch# show ipv6 dhcp

This device's DUID is 0001000111A8040D001FC6D1D47B.

Switch#
```

В данном примере показано, как отобразить настройки DHCPv6 для интерфейса VLAN 1, если на VLAN 1 отключена функция DHCPv6.

```
Switch# show ipv6 dhcp interface vlan 1

vlan 1 is not in DHCPv6 mode.

Switch#
```

В данном примере показано, как отобразить настройки DHCPv6 для всех VLAN. Отображаются только те VLAN, на которых включена функция DHCPv6.

```
Switch# show ipv6 dhcp interface

vlan 1 is in client mode
  State is OPEN
  List of known servers:
    Reachable via address: FE80::200:11FF:FE22:3344
  Configuration parameters:
    IA PD: IA ID 1, T1 40, T2 64
    Prefix: 2000::/48
           preferred lifetime 80, valid lifetime 100
  Prefix name: yy
  Rapid-Commit: disabled

Switch#
```

24. Команды DHCPv6 Guard

24-1 ipv6 dhcp guard policy

Данная команда используется для создания или изменения политики DHCPv6 Guard Policy. Команда позволяет войти в режим DHCPv6 Guard Configuration Mode. При использовании формы **no** данная команда удалит политику DHCPv6 Guard.

```
ipv6 dhcp guard policy POLICY-NAME
no ipv6 dhcp guard policy
```

Параметры

<i>POLICY-NAME</i>	Укажите имя политики DHCPv6 Guard.
--------------------	------------------------------------

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для создания или изменения политики DHCPv6 Guard Policy. Команда позволяет войти в режим DHCPv6 Guard Configuration Mode. Политики DHCPv6 Guard могут использоваться для блокировки ответов DHCPv6 Reply и сообщений, приходящих с неавторизованного сервера. Сообщения клиента не блокируются.

После создания политики DHCPv6 Guard используйте команду **ipv6 dhcp guard attach-policy** для применения политики на определенном интерфейсе.

Пример

В данном примере показано, как создать политику DHCPv6 Guard.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp guard policy policy1
Switch(config-dhcp-guard)# device-role server
Switch(config-dhcp-guard)# match ipv6 access-list acl1
Switch(config-dhcp-guard)#
```

24-2 device-role

Данная команда используется для указания роли подключенного устройства. При использовании формы **no** данная команда вернется к настройкам по умолчанию.

device-role {client | server}
no device-role

Параметры

client	Укажите, чтобы настроить подключенное устройство в качестве клиента DHCPv6. Все сообщения сервера DHCPv6 на этом порту будут отбрасываться.
server	Укажите, чтобы настроить подключенное устройство в качестве сервера DHCPv6. Все сообщения сервера DHCPv6 на этом порту будут приниматься.

По умолчанию

По умолчанию настроена опция **client**.

Режим ввода команды

DHCPv6 Guard Policy Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для указания роли подключенного устройства. По умолчанию устройство выполняет роль клиента, и все сообщения сервера DHCPv6, приходящие на порт, будут отбрасываться. Если настроить устройство в качестве сервера, сообщения сервера DHCPv6 будут разрешены на данном порту.

Пример

В данном примере показано, как создать политику DHCPv6 Guard и настроить устройство в качестве сервера.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp guard policy dhcpguard1
Switch(config-dhcp-guard)# device-role server
Switch(config-dhcp-guard)#
```

24-3 match ipv6 access-list

Данная команда используется для проверки IPv6-адреса источника в сообщениях сервера. При использовании формы **no** данная команда отключит проверку.

match ipv6 access-list IPV6-ACCESS-LIST-NAME
no match ipv6 access-list

Параметры

IPV6-ACCESS-LIST-NAME	Укажите список доступа IPv6, с которым необходимо сверяться.
------------------------------	--

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

DHCPv6 Guard Policy Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для фильтрации DHCPv6-сообщений сервера на основе IP-адреса источника. Если не настроена команда **match ipv6 access-list**, все сообщения сервера будут игнорироваться. Список доступа настраивается с помощью команды **ipv6 access-list**.

Пример

В 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)#
```

24-4 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 vlan {add | remove} VLAN-ID-LIST]  
no ipv6 dhcp guard attach-policy
```

Параметры

<i>POLICY-NAME</i>	Укажите список доступа IPv6, с которым необходимо сверяться.
vlan add <i>VLAN-ID-LIST</i>	(Опционально) Укажите VLAN для проверки. Если VLAN не указана, проверяться будут все VLAN.
vlan remove <i>VLAN-ID-LIST</i>	(Опционально) Укажите VLAN, для которой необходимо отменить проверку.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для применения политики DHCPv6 Guard на интерфейсе. Политики DHCPv6 Guard используются для блокировки DHCPv6-сообщений сервера или фильтрации сообщений сервера на основе IP-адреса источника. Если имя политики не указано, то политика по умолчанию настроит устройство в качестве клиента.

Пример

В данном примере показано, как применить политику DHCPv6 Guard «pol1» для Ethernet 1/0/3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ipv6 dhcp guard attach-policy pol1
Switch(config-if)#
```

24-5 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

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Если указано имя политики, то отображаться будет информация только для нее. Если имя политики не указано, отображаться будет информация для всех политик.

Пример

В данном примере показано, как включить отображение информации для всех политик.

```
Switch# show ipv6 dhcp guard policy

DHCP guard policy: default
  Device Role: DHCP client
  Target: eth1/0/3

DHCP guard policy: test1
  Device Role: DHCP server
  Source Address Match Access List: acl1
  Target: eth1/0/1

Switch#
```

Отображаемые параметры

Device Role	Роль устройства. Ролью может быть клиент или сервер.
Target	Название интерфейса.
Source Address Match Access List	Список доступа IPv6 определенной политики.

25. Команды DHCPv6 Relay

25-1 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Чтобы включить на интерфейсе функцию DHCPv6 Relay, настройте адрес Relay Destination при помощи команды **ipv6 dhcp relay destination**. Чтобы удалить адрес Relay, используйте команду **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 данном примере показано, как сконфигурировать адрес Relay Destination на VLAN 1.


```
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)#
```

25-2 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 {default | cid-with-user-define | user-define | expert-udf
[standalone_unit_format {0 | 1}]}**
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. Тип sub-опции: число 1 свидетельствует о том, что тип данного ID – Remote ID.

F02. VLAN ID: входящий VLAN ID в пакете DHCP Client.

F03. ID модуля: ID модуля для автономных коммутаторов – 0.ID модуля для стекированных коммутаторов – Unit ID.

F04. ID порта: номер входящего порта в пакете DHCP Client.

Номера портов начинаются с 1.

F05. MAC-адрес: системный MAC-адрес коммутатора.

cid-with-user-define

Укажите, чтобы использовать CID со строкой, заданной пользователем, в качестве Remote ID. Формат Remote ID представлен ниже:

F01	F02	F03	F04	F05
Sub Type	VLAN ID	Module ID	Port ID	User Defined
1 byte	2 bytes	1 byte	1 byte	Max. 256 bytes

F01. Tun sub-опции: число 2 свидетельствует о том, что тип данного ID – Remote ID.

F02. VLAN ID: входящий VLAN ID в пакете DHCP Client.

F03. ID модуля: ID модуля для автономных коммутаторов – 0.

ID модуля для стекированных коммутаторов – Unit ID.

F04. ID порта: номер входящего порта в пакете DHCP Client.

Номера портов начинаются с 1.

F05. Задать самостоятельно: заданная пользователем строка, настраиваемая при помощи команды **ipv6 dhcp relayremote-id udf**. По умолчанию данное поле не заполнено.

user-define

Укажите, чтобы задать Remote ID самостоятельно. Формат Remote ID представлен ниже:

```

|-----|
| F01          | 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

Укажите, чтобы задать Remote ID самостоятельно. Формат удаленного ID представлен ниже:

```

|-----|
| F01          |
|-----|
| User Defined  |
|-----|
| Max. 256 bytes |
|-----|

```

F01. Задать самостоятельно: произвольная заданная пользователем строка, настраиваемая при помощи команд **ipv6 dhcp relay remote-id format-type**, **ipv6 dhcp relay remote-id profile** и **format string**. По умолчанию данное поле не заполнено.

standalone_unit_format

Укажите Unit ID для автономного коммутатора. Значение по умолчанию – 0.

По умолчанию

Формат DHCPv6 Relay Remote ID по умолчанию – **default**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить sub-опцию Remote ID.

Пример

В данном примере показано, как настроить sub-опцию Remote ID «cid-with-user-define».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id format cid-with-user-define
Switch(config)#
```

25-3 ipv6 dhcp relay remote-id option

Данная команда используется для того, чтобы включить встраивание Relay Agent Remote ID Option 37в ретранслируемых пакетах запроса DHCP IPv6. Используйте форму **no**, чтобы отключить данную функцию.

ipv6 dhcp relay remote-id option
no ipv6 dhcp relay remote-id option

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить встраивание функции DHCPv6 Relay Agent Remote ID Option.

Пример

В данном примере показано, как включить встраивание DHCPv6 Relay Agent Remote ID Option.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id option
Switch(config)#
```

25-4 ipv6 dhcp relay remote-id policy

Данная команда используется для настройки политики перенаправления Option 37 для DHCPv6 Relay Agent. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ipv6 dhcp relay remote-id policy {drop | keep}
no ipv6 dhcp relay remote-id policy
```

Параметры

drop	Укажите, чтобы отбросить пакет, в котором уже есть Relay Agent Remote ID Option 37.
keep	Укажите, чтобы напрямую ретранслировать пакет запроса DHCPv6, в котором уже есть Relay Agent Remote ID Option, на сервер DHCPv6 в неизменном виде.

По умолчанию

Параметр по умолчанию – **keep**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить глобальную политику для пакетов, в которых уже есть Option 37. При выборе политики **drop** полученный от клиента пакет, в котором уже присутствует RelayAgent Remote ID Option, будет отброшен. При выборе политики **keep** коммутатор не будет проверять, присутствует ли в полученном пакете Relay Agent Remote ID Option.

Пример

В данном примере показано, как настроить политику DHCPv6 Relay Agent Remote ID Option так, чтобы пакет был отброшен при наличии в нем Relay Agent Remote ID Option.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id policy drop
Switch(config)#
```

25-5 ipv6 dhcp relay remote-id udf

Используйте данную команду, чтобы настроить User Define Field (UDF) для Remote ID. Используйте форму **no**, чтобы удалить запись UDF.

```
ipv6 dhcp relay remote-id udf {ascii STRING | hex HEX-STRING}
no ipv6 dhcp relay remote-id udf
```

Параметры

ascii <i>STRING</i>	Укажите строку ASCII для UDF Remote ID. Максимально допустимое количество символов – 128.
hex <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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить UDF для Remote ID.

Пример

В данном примере показано, как настроить UDF (строка ASCII) «PARADISE001».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id udf ascii PARADISE001
Switch(config)#
```

В данном примере показано, как настроить UDF (шестнадцатеричная строка) «010c08».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id udf hex 010c08
Switch(config)#
```

25-6 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 командыUser/Privileged EXEC Mode
Любой режим конфигурации**Уровень команды по умолчанию**

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить DHCPv6 DUID устройства. Для отображения настроек DHCPv6 и информации об указанном интерфейсе VLAN используйте команду **show ipv6 dhcp interface**. Если ID интерфейса не указан, будут отображены все интерфейсы, для которых включена функция DHCPv6.

Пример

В данном примере показано, как отобразить настройки DHCPv6 для VLAN 1, если режим DHCPv6 Relay Mode включен.

```
Switch # show ipv6 dhcp interface vlan 1

vlan 1 is in relay mode
  Relay destinations:
    FE80::20A:BBFF:FECC:102 via vlan 2

Switch #
```

В данном примере показано, как отобразить информацию о DHCPv6 для интерфейса VLAN 1, если режим DHCPv6 Mode отключен.

```
Switch# show ipv6 dhcp interface vlan 1

vlan 1 is not in DHCPv6 mode

Switch#
```

25-7 show ipv6 dhcp relay information option

Данная команда используется для отображения настроек DHCPv6 Relay Information Options.

show ipv6 dhcp relay information option

Параметры

Нет

По умолчанию

F01. Tun sub-опции: число 1 свидетельствует о том, что тип данного ID – interface ID.

F02. VLAN ID: входящий VLAN ID в пакете DHCP Client.

cid

Укажите, чтобы использовать CID в качестве interface ID. Формат interface ID показан ниже:

```

|-----|
| F01      | F02      | F03      | F04      |
|-----|-----|-----|-----|
| Sub Type | VLAN ID  | Module ID| Port ID  |
|-----|-----|-----|-----|
| 1 byte   | 2 bytes  | 1 byte   | 1 byte   |
|-----|
    
```

F01. Tun sub-опции: число 2 свидетельствует о том, что тип данного ID – interface ID.

F02. VLAN ID: исходящий 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.

vendor1

Укажите, чтобы использовать vendor 1. Формат interface ID показан ниже:

F01	F02	F03	F04	F05
E	t	h	e	r
(0x45)	(0x74)	(0x68)	(0x65)	(0x72)
1 byte	1 byte	1 byte	1 byte	1 byte
F06	F07	F08	F09	F10
n	e	t	Chassis ID	/
(0x6E)	(0x65)	(0x74)		(0x2F)
1 byte	1 byte	1 byte	1-2 byte	1 byte
F11	F12	F13	F14	F15
0	/	Port	:	vlan
(0x30)	(0x2F)	Number	(0x2A)	
1 byte	1 byte	1-2 byte	1 byte	1-4 byte
F16	F17	F18	F19	F20
.	0	Space	System	/
(0x2E)	(0x30)	(0x20)	Name	(0x2F)
1 byte	1 byte	1 byte	1-128 byte	1 byte
F21	F22	F23	F24	F25
0	/	0	/	Chassis ID
(0x30)	(0x2F)	(0x30)	(0x2F)	
1 byte	1 byte	1 byte	1 byte	1-2 byte
F26	F27	F28	F29	
/	0	/	Port	
(0x2F)	(0x30)	(0x2F)	Number	
1 byte	1 bytes	1 byte	1-2 byte	

F01. E: код ASCII – 0x45.**F02.** t: код ASCII – 0x74. **F03.** h: код ASCII – 0x68.**F04.** e: код ASCII – 0x65.**F05.** r: код ASCII – 0x72.
F06. n: код ASCII – 0x6E **F07.** e: код ASCII – 0x65.**F08.** t: код ASCII – 0x74.

F09. ID шасси: номер шасси. ID шасси для автономных коммутаторов – 0. ID шасси для стекированных коммутаторов – Unit ID.

F10. Косая черта (/): код ASCII – 0x2F.

F11. 0: Код ASCII – 0x30.

F12. Косая черта (/): код ASCII – 0x2F.

F13. *Номер порта:* номер входящего порта в пакете DHCP Client.

F14. *Двоеточие (:):* код ASCII – 0x3A.

F15. *svlan:* VLAN ID клиента. Диапазон значений: от 1 до 4094.

F16. *Точка (.):* код ASCII – 0x2E.

F17. *0:* код ASCII – 0x30.

F18. *Пробел:* код ASCII – 0x20.

F19. *Системное имя:* системное имя коммутатора.

F20. *Косая черта (/):* код ASCII – 0x2F.

F21. *0:* Код ASCII – 0x30.

F22. *Косая черта (/):* код ASCII – 0x2F.

F23. *0:* Код ASCII – 0x30.

F24. *Косая черта (/):* код ASCII – 0x2F.

F25. *ID шасси:* номер шасси. ID шасси для автономных коммутаторов – 0. ID шасси для стекированных коммутаторов – Unit ID.

F26. *Косая черта (/):* код ASCII – 0x2F.

F27. *0:* Код ASCII – 0x30.

F28. *Косая черта (/):* код ASCII – 0x2F.

F29. *Номер порта:* номер входящего порта в пакете DHCP Client.

expert-udf

Укажите, чтобы задать interface ID самостоятельно. Формат interface ID представлен ниже:

```
|-----|
| F01    |
|-----|
| User Defined |
|-----|
| Max. 255 bytes |
|-----|
```

F01. *Задать самостоятельно:* заданная пользователем строка, настраиваемая при помощи команд **ipv6 dhcp relay interface-id format-type expert-udf**, **ipv6 dhcp relay interface-id profile** и **format string**. По умолчанию данное поле не заполнено.

По умолчанию

Формат DHCPv6 Relay interface ID по умолчанию – **default**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить sub-опцию interface ID.

Пример

В данном примере показано, как настроить sub-опцию interface ID «cid».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay interface-id format cid
Switch(config)#
```

25-9 ipv6 dhcp relay interface-id option

Данная команда используется для того, чтобы включить встраивание Relay Agent Interface ID Option 18 в ретранслируемых пакетах запроса DHCP IPv6. Используйте форму **no**, чтобы отключить данную функцию.

```
ipv6 dhcp relay interface-id option
no ipv6 dhcp relay interface-id option
```

Параметры

Нет

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить встраивание функции DHCPv6 Relay Agent Interface ID Option.

Пример

В данном примере показано, как включить встраивание DHCPv6 Relay Agent Interface ID Option.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay interace-id option
Switch(config)#
```

25-10ipv6 dhcp relay interface-id policy

Данная команда используется для настройки политики перенаправления Option 18 для DHCPv6 RelayAgent. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ipv6 dhcp relay interface-id policy {drop | keep}
no ipv6 dhcp relay interface-id policy
```

Параметры

drop	Укажите, чтобы отбросить пакет, в котором уже есть Relay Agent Interface ID Option 18.
keep	Укажите, чтобы напрямую ретранслировать пакет запроса DHCPv6, в котором уже есть Relay Agent Interface ID Option, на сервер DHCPv6 в неизменном виде.

По умолчанию

Параметр по умолчанию – **keep**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить глобальную политику для пакетов, в которых уже есть Option 18. При выборе политики **drop** полученный от клиента пакет, в котором уже присутствует Relay Agent Interface ID Option, будет отброшен. При выборе политики **keep** коммутатор не будет проверять, присутствует ли в полученном пакете Relay Agent Interface ID Option.

Пример

В данном примере показано, как настроить политику DHCPv6 Relay Agent Interface ID Option так, чтобы пакет был отброшен при наличии в нем Relay Agent Interface ID Option.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay interface-id policy drop
Switch(config)#
```

25- 11 ipv6 dhcp local-relay vlan

Данная команда используется для включения DHCPv6 Local Relay на VLAN или группе VLAN.Используйте форму **no**, чтобы отключить данную функцию.

```
ipv6 dhcp local-relay vlan VLAN-ID [, | -]
no ipv6 dhcp local-relay vlan VLAN-ID [, | -]
```

Параметры

VLAN-ID	Укажите ID VLAN, которую необходимо настроить.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для настройки функции DHCPv6 Local Relay.

Если функция DHCPv6 Local Relay включена, коммутатор добавит Option 37 и Option 18 в пакеты запроса клиента.

Если проверка Option 37 включена, коммутатор проверит пакет запроса, полученный от клиента, при этом пакет, содержащий Option 37, в соответствии с функцией DHCPv6 Relay будет отброшен.

Если проверка Option 37 отключена, функция Local Relay будет добавлять Option 37 в пакет запроса вне зависимости от того, включена Option 37 или выключена.

Функция DHCPv6 Local Relay напрямую передаст пакет от сервера клиенту.



Примечание: если на интерфейсе отключена команда `ipv6 dhcp relay enable`, ретрансляция и локальная ретрансляция полученных пакетов DHCPv6 выполняться не будет.

Пример

В данном примере показано, как включить функцию DHCPv6 Local Relay на VLAN 100.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp local-relay vlan 100
Switch(config)#
```

25- 12 ipv6 dhcp relay enable

Данная команда используется для включения функции DHCPv6 Relay на порту. Используйте форму **no**, чтобы отключить данную функцию.

ipv6 dhcp relay enable
no ipv6 dhcp relay enable

Параметры

Нет

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить функцию DHCPv6 Relay для каждого порта.

Пример

В данном примере показано, как отключить функцию DHCPv6 Relay на порту Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#no ipv6 dhcp relay enable
Switch(config-if)#
```

25-13 ipv6 dhcp relay remote-id profile

Данная команда используется, чтобы создать новый профиль для DHCPv6 Relay Option 37 и войти в режим DHCPv6 Profile Configuration Mode. Используйте форму **no**, чтобы удалить профиль.

ipv6 dhcp relay remote-id profile NAME
no ipv6 dhcp relay remote-id profile NAME

Параметры

<i>NAME</i>	Укажите имя профиля. Максимально допустимое количество символов – 32. Максимально допустимое количество записей в профиле – 6.
-------------	--

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы создать/удалить профиль для DHCPv6 Relay Option 37, а также войти в режим DHCPv6 Profile Configuration Mode.

Пример

В данном примере показано, как создать профиль «profile1» для DHCPv6 Relay Option 37.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay remote-id profile profile1
Switch(config-dhcp-profile)#
```

25-14 ipv6 dhcp relay interface-id profile

Данная команда используется для создания нового профиля для DHCPv6 Relay Option 18 и входа в режим DHCPv6 Profile Configuration Mode. Используйте форму **no**, чтобы удалить профиль.

ipv6 dhcp relay interface-id profile NAME
no ipv6 dhcp relay interface-id profile NAME

Параметры

<i>NAME</i>	Укажите имя профиля. Максимально допустимое количество символов – 32. Максимально допустимое количество записей в профиле – 6.
-------------	--

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы создать/удалить профиль для DHCPv6 Relay Option 18, а также войти в режим DHCPv6 Profile Configuration Mode.

Пример

В данном примере показано, как создать профиль «profile 2» для DHCPv6 Relay Option 18.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay interface-id profile profile2
Switch(config-dhcp-profile)#
```

25-15 format string

Данная команда используется для самостоятельного добавления записи Option 18 или Option 37. Используйте форму **no**, чтобы удалить запись.

format string *STRING*
no format string

Параметры

string	<p>Укажите формат DHCP Option 82. Максимально допустимое количество символов – 255.</p> <p>Ниже представлены правила конфигурирования данного параметра:</p> <ul style="list-style-type: none"> • Параметр может содержать шестнадцатеричные значения, строку ASCII или любую комбинацию шестнадцатеричных значений и строки ASCII. Строка ASCII должна быть заключена в кавычки (" "), например: "Ethernet". Символы ASCII вне кавычек будут распознаны как шестнадцатеричные значения. • Отформатированная ключевая строка – строка, которую необходимо преобразовать до того, как она будет запакетирована. Отформатированная ключевая строка может содержать как строки ASCII, так и шестнадцатеричные значения, например: "%\$1-32keyword": <p>% – указывает на то, что строка, следующая за символом, является отформатированной ключевой строкой.</p> <p>\$ 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.</p> <p>\$ означает заполнение начального пробела (0x20).</p> <p>0 означает заполнение начального нуля (0). Заполнение начального нуля (0) – настройка по умолчанию.</p> <p>1-32 – (опционально) индикатор длины. Данная опция указывает, сколько символов или байтов должна занимать преобразованная ключевая строка. Если фактическая длина преобразованной ключевой строки меньше длины, предусмотренной данной опцией, будет использован индикатор заполнения. В других случаях будет использована фактическая длина строки.</p> <p>keyword – указывает на то, что ключевое слово будет преобразовано на основе фактического</p>
---------------	--

значения системы. Следующие ключевые слова указывают на то, 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 при помощи специальной команды (например, **ip dhcp relay information option mac-format case**). При использовании шестнадцатеричных значений MAC-адрес будет сформирован в шестнадцатеричном виде.

sysmac: системный MAC-адрес. Могут быть использованы строка ASCII или шестнадцатеричные значения. При использовании строки ASCII MAC-адрес может быть сформирован при помощи команд CLI (например, **ip dhcp relay information option mac-format case**). При использовании шестнадцатеричных значений MAC-адрес будет сформирован в шестнадцатеричном виде.

unit: Unit ID коммутатора в стеке. Могут быть использованы строка ASCII или шестнадцатеричные значения. Для нестекированных коммутаторов Unit ID указывается при помощи команды **ipv6 dhcp relay remote-id format expert_udf [standalone_unit_format {0 | 1}]**, а также команды **ipv6 dhcp relay interface-id format 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

Параметр по умолчанию – **keep**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить запись задаваемой пользователем Option 18 или Option 37.

Пример

В данном примере показано, как настроить запись задаваемой пользователем Option 18.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay interface-id profile profile2
Switch(config-dhcp-profile)#format string "Ethernet %unit:/0/ %port:\:%sysname:%05vlan"
Switch(config-dhcp-profile)#
```

25- 16 ipv6 dhcp relay information option mac-format case

Данная команда используется для настройки формата MAC-адреса, задаваемого пользователем в профиле DHCPv6 Option 18 или Option 37. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ipv6 dhcp relay information option mac-format case {lowercase | uppercase} delimiter {hyphen |
colon | dot | none} number {1 | 2 | 5}
no ipv6 dhcp relay information option mac-format case
```

Параметры

lowercase	Укажите, чтобы использовать нижний регистр при записи MAC-адреса Option 18 или Option 37 для задаваемого пользователем профиля: aa-bb-cc-dd-ee-ff.
uppercase	Укажите, чтобы использовать верхний регистр при записи MAC-адреса Option 18 или Option 37 для задаваемого пользователем профиля: AA-BB-CC-DD-EE-FF.
hyphen	Укажите, чтобы использовать «-» в качестве разделителя данных: AA-BB-CC-DD-EE-FF.
colon	Укажите, чтобы использовать «:» в качестве разделителя данных: AA:BB:CC:DD:EE:FF.
dot	Укажите, чтобы использовать «.» в качестве разделителя данных: AA.BB.CC.DD.EE.FF.
none	Укажите для ввода данных без разделителя: AABCCDDEEFF.
number	Укажите количество разделителей: 1: один разделитель: AABCC.DDEEFF. 2: два разделителя: AABV.CCDD.EEFF. 5: множество разделителей: AA.BB.CC.DD.EE.FF. Если указан параметр none , параметр number будет недействителен.

По умолчанию

Параметр регистра MAC-адреса аутентификации по умолчанию – **uppercase**.

Параметр разделителя MAC-адреса аутентификации по умолчанию – **none**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить формат MAC-адреса, задаваемого пользователем в профиле Option 18 или Option 37.

Пример

В данном примере показано, как настроить формат MAC-адреса, задаваемого пользователем в профиле 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)#
```

25- 17 show ipv6 dhcp relay information option mac-format

Данная команда используется для отображения формата MAC-адреса в профиле Option 18 и Option 37.

```
show ipv6 dhcp relay information option mac-format
```

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить формат MAC-адреса в профиле Option 18 и Option 37.

Пример

В данном примере показано, как отобразить формат MAC-адреса в профиле 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#
```

25- 18 ipv6 dhcp relay remote-id format-type expert-udf

Данная команда используется для настройки строки Option 37 expert UDF на порту. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ipv6 dhcp relay remote-id format-type expert-udf STRING
no ipv6 dhcp relay remote-id format-type expert-udf
```

Параметры

<i>STRING</i>	Укажите имя профиля Option 37.
---------------	--------------------------------

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить строку Option 37 expert UDF на порту.

Пример

В данном примере показано, как настроить Option 37 на порту Ethernet 1/0/1, выбрав профиль «profile1».

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#ipv6 dhcp relay remote-id format-type expert-udf profile1
Switch(config-if)#
```

25- 19 ipv6 dhcp relay interface-id format-type expert-udf

Данная команда используется для настройки строки Option 18 expert UDF на порту. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ipv6 dhcp relay interface-id format-type expert-udf *STRING*
no ipv6 dhcp relay interface-id format-type expert-udf

Параметры

<i>STRING</i>	Укажите имя профиля Option 18.
---------------	--------------------------------

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить строку Option 18 expert UDF на порту.

Пример

В данном примере показано, как настроить Option 18 на порту Ethernet 1/0/1, выбрав профиль «profile2».

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#ipv6 dhcp relay interface-id format-type expert-udf profile2
Switch(config-if)#
```

25-20 show ipv6 dhcp relay interface-id profile

Данная команда используется для отображения профилей Option 18.

show ipv6 dhcp relay interface-id profile

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить профили Option 18.

Пример

В данном примере показано, как отобразить профили Option 18.

```
Switch#show ipv6 dhcp relay interface-id profile

Option18 Profile name: profile2
Format string: "Ethernet %unit:/0/ %port:\:%sysname:%05svlan"

Total Entries:1

Switch#
```

25-21 show ipv6 dhcp relay remote-id profile

Данная команда используется для отображения профилей Option 37.

show ipv6 dhcp relay remote-id profile

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить профили Option 37.

Пример

В данном примере показано, как отобразить профили Option 37.

```
Switch#show ipv6 dhcp relay remote-id profile

Option37 Profile name: profile1
Format string: "Ethernet %unit:/0/ %port:\:%sysname:%05svlan"

Total Entries:1

Switch#
```

26. Команды DHCPv6 Server

26-1 address prefix

Данная команда используется для указания префикса адреса, который будет присвоен клиенту. Используйте форму **no**, чтобы удалить префикс адреса.

```
address prefix IPV6-PREFIX/PREFIX-LENGTH [lifetime VALID-LIFETIME PREFERRED-LIFETIME]
no address prefix
```

Параметры

<i>IPV6-PREFIX</i>	Укажите префикс IPv6-адреса, который необходимо присвоить клиенту.
<i>PREFIX-LENGTH</i>	Укажите длину префикса IPv6-адреса.
lifetime <i>VALID-LIFETIME</i>	(Опционально) Укажите значение Valid Lifetime (допустимое время жизни) для префикса адреса в секундах. Значение Valid Lifetime должно превышать значение Preferred Lifetime (предпочтительное время жизни). Доступный диапазон значений: от 60 до 4294967295 или до бесконечности. Если значение Lifetime не задано, устанавливается значение ValidLifetime по умолчанию – 2592000 секунд (30 дней).
<i>PREFERRED-LIFETIME</i>	(Опционально) Укажите значение Preferred Lifetime для префикса адреса в секундах. Доступный диапазон значений: от 60 до 4294967295 или до бесконечности. Если значение Lifetime не задано, устанавливается значение по умолчанию – 604800 секунд (7 дней).

По умолчанию

Нет

Режим ввода команды

DHCPv6 Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить префикс адреса в пуле IPv6 DHCP. В DHCPv6-пуле можно настроить только один префикс адреса. Последующая команда будет замещать предыдущую.

Получив запрос от клиента, сервер проверит пул IPv6 DHCP, ассоциированный с получающим интерфейсом. Если статические записи привязки адреса настроены так, чтобы присваивать адрес запрашивающему клиенту, будет присвоен адрес статической привязки. Иначе сервер присвоит адрес из префикса адреса, указанного для пула IPv6 DHCP.

Пример

В данном примере показано, как настроить префикс адреса 2001:0DB8::0/64 для пула IPv6 DHCP «pool1».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# address prefix 2001:0DB8::0/64 lifetime 200 100
Switch(config-dhcp)#
```

26-2 address-assignment

Данная команда используется для указания адреса, который необходимо присвоить обозначенному клиенту. Используйте форму **no**, чтобы удалить адрес статической привязки.

address-assignment *IPV6-ADDRESS/PREFIX-LENGTH CLIENT-DUID* [**iaid** *IAID*] [**lifetime** *VALID-LIFETIME PREFERRED-LIFETIME*]

no address-assignment *IPV6-ADDRESS/PREFIX-LENGTH*

Параметры

<i>IPV6-PREFIX</i>	Укажите IPv6-адрес, который необходимо присвоить обозначенному клиенту.
<i>PREFIX-LENGTH CLIENT-DUID</i>	Укажите длину IPv6-префикса. Укажите DHCP Unique Identifier (DUID) клиента, которому необходимо присвоить адрес.
iaid <i>IAID</i>	(Опционально) Укажите Identity Association Identifier (IAID). IAID используется для обозначения серии Non-Temporary Addresses (IANA), присвоенных клиенту.
lifetime <i>VALID-LIFETIME</i>	(Опционально) Укажите значение Valid Lifetime (допустимое время жизни) для адреса в секундах. Значение Valid Lifetime должно превышать значение Preferred Lifetime (предпочтительное время жизни). Доступный диапазон значений: от 60 до 4294967295 или до бесконечности. Если значение Lifetime для адреса не задано, устанавливается значение Valid Lifetime по умолчанию – значение Valid Lifetime для пула.
<i>PREFERRED-LIFETIME</i>	(Опционально) Укажите значение Preferred Lifetime для адреса в секундах. Доступный диапазон значений: от 60 до 4294967295 или до бесконечности. Если значение Lifetime для адреса не задано, устанавливается значение Preferred Lifetime по умолчанию – значение Preferred Lifetime для пула.

По умолчанию

Нет

Режим ввода команды

DHCPv6 Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить статическую запись привязки адреса так, чтобы она указывала адрес, который необходимо присвоить обозначенному клиенту.

Получив запрос от клиента, сервер проверит пул IPv6 DHCP, ассоциированный с полученным интерфейсом. Если сообщение Request содержит опцию IANA и имеются свободные статические записи, настроенные с IAID и соответствующие DUID и IAID сообщения, соответствующая запись будет присвоена. Если соответствующая запись отсутствует, но имеются свободные статические записи без указанных IAID, которые соответствуют DUID сообщения, на соответствующую запись будет отправлен ответ.

При отсутствии соответствующих записей клиенту будет присвоен адрес из префикса адреса, указанного в пуле IPv6 DHCP.

Пример

В данном примере показано, как настроить статическую запись привязки адреса в пуле IPv6 DHCP «pool1» и ассоциировать пул IPv6 DHCP с VLAN 100.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(dhcpv6-config)# address-assignment 2001:0DB8::1:2 000300010506BBCCDDEE
Switch(dhcpv6-config)# exit
Switch(config)# interface vlan 100
Switch(dhcpv6-config)# ipv6 dhcp server pool1
Switch(dhcpv6-config)#
```

В данном примере показано, как настроить статическую запись привязки адреса в пуле IPv6 DHCP «pool2» с опцией IAID и ассоциировать пул IPv6 DHCP с VLAN 200.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool2
Switch(dhcpv6-config)# address-assignment 2001:AAB8::2:2 00030001050611223344 iaid 1234
Switch(dhcpv6-config)# exit
Switch(config)# interface vlan 200
Switch(config-if)# ipv6 dhcp server pool2
Switch(config-if)#
```

26-3 clear ipv6 dhcp binding

Данная команда используется для удаления записей привязки DHCPv6-сервера.

```
clear ipv6 dhcp binding {all | IPV6-PREFIX}
```

Параметры

all	Укажите, чтобы удалить все записи привязки.
IPV6-PREFIX	Укажите, чтобы удалить запись привязки по префиксу.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы удалить записи привязки DHCPv6-сервера. При указании IPv6-префикса будет удалена запись привязки к обозначенному клиенту. Если IPv6-префикс не указан, будут удалены все записи привязки. IPv6-префикс будет возвращен в пул, которому изначально был назначен.

Пример

В данном примере показано, как удалить все записи привязки в таблице привязок DHCPv6-сервера.

```
Switch# clear ipv6 dhcp binding all
Switch#
```

26-4 domain-name

Данная команда используется для назначения имени домена запрашивающему DHCPv6-клиенту. Используйте форму **no**, чтобы удалить настройки имени домена.

```
domain-name DOMAIN-NAME
no domain-name
```

Параметры

<i>DOMAIN-NAME</i>	Укажите имя домена.
--------------------	---------------------

По умолчанию

Нет

Режим ввода команды

DHCPv6 Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы назначить имя домена запрашивающему DHCPv6-клиенту. Можно указать только одно имя домена.

Пример

В данном примере показано, как настроить имя домена в пуле DHCPv6-сервера «pool1».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# domain-name v6domain
Switch(config-dhcp)#
```

26-5 dns-server

Данная команда используется для назначения списка серверов DNS IPv6 запрашивающему IPv6-клиенту. Используйте форму **no**, чтобы удалить DNS-сервер из списка серверов.

```
dns-server IPV6-ADDRESS
no dns-server IPV6-ADDRESS
```

Параметры

<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес DNS-сервера.
---------------------	---------------------------------

По умолчанию

Нет

Режим ввода команды

DHCPv6 Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы присвоить IPv6-адрес DNS-сервера запрашивающему DHCPv6-клиенту. Если необходимо присвоить несколько адресов, введите команду несколько раз.

Пример

В данном примере показано, как настроить сервер DNS IPv6 в пуле DHCPv6-сервера «pool1».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# dns-server 2001:0DB8:3000:3000::42
Switch(config-dhcp)#
```

26-6 ipv6 dhcp excluded-address

Данная команда используется для указания IPv6-адресов, которые DHCPv6-сервер не должен присваивать DHCP-клиентам. Используйте форму **no**, чтобы удалить исключенные IPv6-адреса.

```

ipv6 dhcp excluded-address LOW-ADDRESS [HIGH-ADDRESS]
no ipv6 dhcp excluded-address LOW-ADDRESS [HIGH-ADDRESS]

```

Параметры

<i>LOW-ADDRESS</i>	Укажите исключенный IPv6-адрес или первый IPv6-адрес в диапазоне исключенных адресов.
<i>HIGH-ADDRESS</i>	(Опционально) Укажите последний IPv6-адрес в диапазоне исключенных адресов.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Сервер DHCPv6 предполагает, что клиенту может быть присвоен любой адрес (кроме IPv6-адреса коммутатора). Используйте данную команду, чтобы исключить присвоение одного IPv6-адреса или диапазона IPv6-адресов. Исключенные адреса могут быть присвоены только пулу/пулам адресов.

Пример

В данном примере показано, как исключить IPv6-адрес 3004:DB8::1:10.

```

Switch# configure terminal
Switch(config)# ipv6 dhcp excluded-address 3004:DB8::1:10
Switch(config)#

```

26-7 ipv6 dhcp pool

Данная команда используется для входа в режим DHCP Pool Configuration Mode и настройки пула IPv6 DHCP. Используйте форму **no**, чтобы удалить пул IPv6 DHCP.

```

ipv6 dhcp pool POOL-NAME
no ipv6 dhcp pool POOL-NAME

```

Параметры

<i>POOL-NAME</i>	Укажите имя пула адресов. Максимально допустимое количество символов – 12.
------------------	--

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы войти в режим IPv6 DHCP Pool Configuration Mode и настроить пул IPv6 DHCP. Используйте команду **ipv6 dhcp server**, чтобы включить DHCP IPv6 Server Service на интерфейсе и указать пул IPv6 DHCP, используемый для обслуживания DHCP-запроса, полученного на интерфейсе.

Пример

В данном примере показано, как настроить пул адресов «pool1».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)#
```

26-8 ipv6 dhcp server

Данная команда используется для включения DHCP IPv6 Server Service на интерфейсе. Используйте форму **no**, чтобы отключить DHCP IPv6 Server Service.

```
ipv6 dhcp server POOL-NAME [rapid-commit]
no ipv6 dhcp server
```

Параметры

<i>POOL-NAME</i>	Укажите имя пула IPv6 DHCP, обслуживающего запрос, полученный на интерфейсе.
rapid-commit	(Опционально) Укажите, чтобы получать сетевые настройки от DHCP-сервера посредством быстрого обмена двумя сообщениями вместо стандартных четырех между Requesting Router (RR) и Delegating Router (DR). По умолчанию обмен двумя сообщениями отключен.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить DHCP для IPv6 Server Service на указанном интерфейсе.

Один пул IPv6 DHCP можно ассоциировать с несколькими интерфейсами, при этом с одним интерфейсом можно ассоциировать только один пул IPv6 DHCP. Перед ассоциированием пул необходимо настроить. Для IPv6 Client функции DHCP-Server DHCP-Relay несовместимы на одном интерфейсе.

Стандартный обмен сообщениями между маршрутизаторами DR и RR включает в себя четыре типа сообщений: *SOLICIT*, *ADVERTISE*, *REQUEST* и *REPLY*. При использовании параметра **rapid-commit** маршрутизаторы обмениваются двумя сообщениями вместо четырех. В этом случае маршрутизатор RR отправит маршрутизатору DR сообщение *SOLICIT*, в котором уведомит его о возможности пропустить получение сообщения *ADVERTISE* и отправку сообщения *REQUEST* и перейти непосредственно к получению сообщения *REPLY* от маршрутизатора DR. В сообщении *REPLY* содержится информация по сетевым настройкам.

Для корректной работы данного функционала необходимо включить параметр **rapid-commit** и на DR, и на RR.

Пример

В данном примере показано, как создать DHCP-пул «pool1» и использовать его для передачи префиксов, включив DHCP IPv6 Server Service на интерфейсе VLAN 100.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# exit
Switch(config)# interface vlan 100
Switch(config-if)# ipv6 dhcp server pool1
Switch(config-if)#
```

26-9 ipv6 local pool

Данная команда используется для настройки локального пула IPv6-префиксов. Используйте форму **no**, чтобы удалить пул.

ipv6 local pool *POOL-NAME* *IPV6-PREFIX/PREFIX-LENGTH* *ASSIGNED-LENGTH*
no ipv6 local pool *POOL-NAME*

Параметры

<i>POOL-NAME</i>	Укажите имя локального пула IPv6-префиксов. Максимально допустимое количество символов – 12.
<i>IPV6-PREFIX</i>	Укажите адрес IPv6-префикса в локальном пуле.
<i>PREFIX-LENGTH</i>	Укажите длину IPv6-префикса в локальном пуле.
<i>ASSIGNED-LENGTH</i>	Укажите длину префикса, который необходимо делегировать из пула пользователю. Заданная длина не может быть меньше длины префикса.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Локальный пул IPv6-префиксов определяет блок префиксов. Настройте пул с префиксами, которые пересекаются с другими пулами. Чтобы изменить префикс в локальном пуле, удалите локальный пул, а затем создайте его заново. Все префиксы данного пула, которые уже были распределены, будут свободны.

Пример

В данном примере показано, как создать локальный пул IPv6-префиксов «prefix-pool» и использовать локальный пул в DHCP-пуле «pool1».

```
Switch# configure terminal
Switch(config)# ipv6 local pool prefix-pool 3004:DB8::/48 64
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# prefix-delegation pool prefix-pool lifetime 300 200
Switch(config-dhcp)#
```

26- 10 prefix-delegation

Данная команда используется для указания префикса, который необходимо делегировать обозначенному клиенту. Используйте форму **no**, чтобы удалить префикс статической привязки.

prefix-delegation *IPV6-PREFIX/PREFIX-LENGTH CLIENT-DUID* [**iaid** *IAID*] [**lifetime** *VALID-LIFE-TIME PREFERRED-LIFETIME*]

no prefix-delegation *IPV6-PREFIX/PREFIX-LENGTH*

Параметры

<i>IPV6-PREFIX</i>	Укажите IPv6-префикс, который необходимо делегировать обозначенному клиенту.
<i>PREFIX-LENGTH CLIENT-DUID</i>	Укажите длину IPv6-префикса. Укажите DHCP Unique Identifier (DUID) клиента, которому необходимо делегировать префикс.
iaid <i>IAID</i>	(Опционально) Укажите Identity Association Identifier (IAID). IAID используется для обозначения серии префиксов, присвоенных Requesting Router (RR).
lifetime <i>VALID-LIFE-TIME</i>	(Опционально) Укажите значение Valid Lifetime (допустимое время жизни) для префикса в секундах. Значение Valid Lifetime должно превышать значение Preferred Lifetime (предпочтительное время жизни). Доступный диапазон значений: от 60 до 4294967295 или до бесконечности. Если значение Lifetime не задано, устанавливается значение Valid Lifetime по умолчанию – 2592000 секунд (30 дней).
<i>PREFERRED-LIFETIME</i>	(Опционально) Укажите значение Preferred Lifetime для префикса в секундах. Доступный диапазон значений: от 60

до 4294967295 или до бесконечности. Если значение Lifetime не задано, устанавливается значение Preferred Lifetime по умолчанию – 604800 секунд (7 дней).

По умолчанию

Нет

Режим ввода команды

DHCPv6 Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить статическую запись привязки префикса так, чтобы она указывала префикс, который необходимо делегировать обозначенному клиенту. Для клиента можно настроить несколько статических записей привязки префиксов или IAPD.

Получив запрос от клиента, сервер проверит пул IPv6 DHCP, ассоциированный с полученным интерфейсом. Если сообщение request содержит опцию IAPD и имеются свободные статические записи, настроенные с IAID и соответствующие DUID и IAID сообщения, будут делегированы все соответствующие записи. Если соответствующие записи отсутствуют, но имеются свободные статические записи без указанных IAID, которые соответствуют DUID сообщения, на соответствующую запись будет отправлен ответ. Если в сообщении request отсутствует опция IAID, а в наличии есть свободные статические записи без указанных IAID, которые соответствуют DUID сообщения, на соответствующие записи будет отправлен ответ.

При отсутствии соответствующих записей клиенту будет делегирован префикс из локального пула IPv6-префиксов, указанного в пуле IPv6 DHCP.

Пример

В данном примере показано, как настроить статическую запись привязки префикса в пуле IPv6 DHCP «pool1» и ассоциировать данный пул с VLAN 100.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# prefix-delegation 2001:0DB8::/64 000300010506BCCDDEE
Switch(config-dhcp)# exit
Switch(config)# interface vlan 100
Switch(config-if)# ipv6 dhcp server pool1
Switch(config-if)#
```

26-11 prefix-delegation pool

Данная команда используется для указания локального пула IPv6-префиксов, из которого префиксы могут быть делегированы. Используйте форму **no**, чтобы удалить локальный пул IPv6-префиксов.

prefix-delegation pool POOL-NAME [lifetime VALID-LIFETIME PREFERRED-LIFETIME]
no prefix-delegation pool POOL-NAME

Параметры

<i>POOL-NAME</i>	Укажите имя локального пула IPv6-префиксов.
lifetime <i>VALID-LIFETIME</i>	(Опционально) Укажите значение Valid Lifetime (допустимое время жизни) для префикса в секундах. Значение Valid Lifetime должно превышать значение Preferred Lifetime (предпочтительное время жизни). Доступный диапазон значений: от 60 до 4294967295 или до бесконечности. Если значение Lifetime не задано, устанавливается значение Valid Lifetime по умолчанию – 2592000 секунд (30 дней).
<i>PREFERRED-LIFETIME</i>	(Опционально) Укажите значение Preferred Lifetime для префикса в секундах. Доступный диапазон значений: от 60 до 4294967295 или до бесконечности. Если значение Lifetime не задано, устанавливается значение Preferred Lifetime по умолчанию – 604800 секунд (7 дней).

По умолчанию

Нет

Режим ввода команды

DHCPv6 Pool Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для указания локального пула IPv6-префиксов в пуле IPv6 DHCP, чтобы делегировать префикс клиентам, обслуживаемым DHCP-пулом. В пуле IPv6 DHCP можно указать только один локальный пул IPv6-префиксов.

Получив запрос от клиента, сервер проверит пул IPv6 DHCP, ассоциированный с полученным интерфейсом. Если статические записи привязки префикса настроены так, чтобы делегировать префикс запрашивающему клиенту, будет делегирован префикс статической привязки. Иначе сервер делегирует префикс из локального пула IPv6-префиксов, указанного для пула IPv6 DHCP.

Пример

В данном примере показано, как настроить локальный пул IPv6-префиксов «prefix-pool», указать данный пул в пуле IPv6 DHCP «pool1» и ассоциировать пул IPv6 DHCP с VLAN 100.

```
Switch# configure terminal
Switch(config)# ipv6 local pool prefix-pool 3004:DB8::/48 64
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# prefix-delegation pool prefix-pool lifetime 300 200
Switch(config-dhcp)# exit
Switch(config)# interface vlan 100
Switch(config-if)# ipv6 dhcp server pool1
Switch(config-if)#
```

26-12 service ipv6 dhcp

Данная команда используется для включения сервера IPv6 DHCP и Relay Service на коммутаторе. Используйте форму **no** для отключения сервера IPv6 DHCP и Relay Service.

```
service ipv6 dhcp
no service ipv6 dhcp
```

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы глобально включить сервер IPv6 DHCP и Relay Service на коммутаторе. Чтобы настройки вступили в силу, необходимо отключить, а затем снова включить DHCPv6-сервер.

Пример

В данном примере показано, как включить сервер IPv6 DHCP и Relay Service.

```
Switch# configure terminal
Switch(config)# service ipv6 dhcp
Switch(config)#
```

26-13 show ipv6 dhcp

Данная команда используется для отображения настроек DHCPv6 для интерфейсов.

```
show ipv6 dhcp [interface [INTERFACE-ID]]
```

Параметры

<i>INTERFACE-ID</i>	(Опционально) Укажите интерфейс VLAN, для которого необходимо отобразить настройки DHC Pv6.
---------------------	---

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить DHCPv6 DUID устройства. Используйте команду **show ipv6 dhcp interface**, чтобы отобразить настройки DHCPv6 для интерфейсов. Если ID интерфейса не указан, будут отображены все интерфейсы, на которых включена функция DHCPv6.

Пример

В данном примере показано, как отобразить информацию о DHCPv6 для интерфейса VLAN 1, если на VLAN 1 отключен DHCPv6.

```
Switch# show ipv6 dhcp interface vlan 1

vlan 1 is not in DHCPv6 mode

Switch#
```

В данном примере показано, как отобразить DHCPv6 client для интерфейса VLAN 1, если на VLAN 1 включен DHCPv6-сервер.

```
Switch# show ipv6 dhcp interface vlan 1

vlan 1 is in server mode
 IPv6 DHCP pool is test
 Preference value: 0
 Hint from client: ignored
 Rapid-Commit is disabled

Switch#
```

26-14 show ipv6 dhcp binding

Данная команда используется для отображения записи привязки IPv6-префикса.

show ipv6 dhcp binding [IPV6-PREFIX]

Параметры

<i>IPV6-PREFIX</i>	(Опционально) Укажите, чтобы отобразить запись привязки.
--------------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

При использовании данной команды без указания параметра *IPV6-PREFIX* будут отображены все привязки префикса DHCP Pv6 клиента в таблице привязок. При указании параметра *IPV6-PREFIX* будет отображена только привязка префикса указанного клиента.

Пример

В данном примере показано, как отобразить запись привязки IPv6-префикса.

```
Switch# show ipv6 dhcp binding

Client DUID : 00030001aabbcd000001
      address: 1234::2
      preferred lifetime 200 ,valid lifetime 300

Client DUID : 00030001aabbcd000000
      address: 1234::3
      preferred lifetime 200 ,valid lifetime 300

Client DUID : 00030001aabbcd000002
      address: 1234::4
      preferred lifetime 200 ,valid lifetime 300

Total Entries: 3

Switch#
```

26-15 show ipv6 dhcp pool

Данная команда используется для отображения информации о настройках пула DHCPv6-сервера.

```
show ipv6 dhcp pool [POOL-NAME]
```

Параметры

<i>POOL-NAME</i>	(Опционально) Укажите, чтобы отобразить пул IPv6 DHCP.
------------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

При использовании данной команды без указания параметра *POOL-NAME* будет отображена информация о настройках всех пулов DHCPv6-сервера. При указании параметра *POOL-NAME* будет отображена информация только об указанном пуле.

Пример

В данном примере показано, как отобразить информацию о DHCPv6-пуле.

```
Switch# show ipv6 dhcp pool

DHCPv6 pool: pool1
  Static bindings:
    Binding for client 00030001aabbcd000080
    IA PD: IA ID 0x0001
    Prefix: 3000:0:300::/48
    preferred lifetime 604800, valid lifetime 2592000
  Prefix delegation pool: abc
    preferred lifetime 604800, valid lifetime 2592000
  DNS server: 2345::2
  Domain name: pool1.com
  Active clients: 0

DHCPv6 pool: pool2
  DNS server: 6000::2
  DNS server: 6000::9
  Domain name: pool2.com
  Active clients: 0

DHCPv6 pool: test
  Static bindings:
    Binding for client 00030001aabbcd001234
    IA NA: IA ID not specified
    Address: 1234::1234
    preferred lifetime 604800, valid lifetime 2592000
  Address prefix: 1234::/64
    preferred lifetime 200, valid lifetime 300
  DNS server:
  Domain name:
  Active clients: 3

Switch#
```

Отображаемые параметры

DHCPv6 pool

Имя пула.

Binding for client 000300010002FCA5C01C	Статическая привязка для клиента с DUID 000300010002FCA5C01C.
IAPD	Серия префиксов, присвоенных клиенту.
IAID	Идентификатор данной IAPD.
Prefix	Префиксы, которые необходимо делегировать.
preferred lifetime, valid lifetime	Значения Preferred Lifetime и Valid Lifetime для префикса, присвоенные клиенту.
DNS server	Список адресов DNS-сервера.
Domain name	Список настроенных DNS-доменов.
Active clients	Общее количество активных клиентов.

26- 16 show ipv6 excluded-address

Данная команда используется для отображения информации о настройках исключенных IPv6-адресов.

show ipv6 excluded-address

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить диапазон исключенных адресов.

Пример

В данном примере показано, как отобразить исключенные адреса.

```
Switch# show ipv6 excluded-address

IPv6 excluded address:
1.3004:DB8::1:10
2.3004:DBB::1:100 - 3004:DBB::1:105

Total Entries: 2

Switch#
```

26-17 show ipv6 local pool

Данная команда используется для отображения информации о настройках локального пула IPv6-префиксов.

show ipv6 local pool [*POOL-NAME*]

Параметры

<i>POOL-NAME</i>	(Опционально) Укажите, чтобы отобразить локальный пул IPv6 префиксов.
------------------	---

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

При использовании данной команды без указания параметра *POOL-NAME* будет отображена информация о настройках всех префиксов. При указании параметра *POOL-NAME* будет отображена информация только о настройках указанного локального пула IPv6-префиксов.

Пример

В данном примере показано, как отобразить информацию о локальном пуле, не указывая имя пула.

```
Switch#show ipv6 local pool

Pool          Prefix                               Free In use
-----
prefix-pool  3004:DB8::/48                       65536 0
-----
Total Entries: 1

Switch#
```

В данном примере показано, как отобразить информацию о локальном пуле «PP1».

```
Prefix is 3004:DB8::/48 assign /64 prefix
1 entries in use, 65536 available, 0 rejected
User          Prefix                               Interface
-----
000300010002FCA5C01C 2003::/64                             vlan 1

Switch#
```


26-18 show ipv6 dhcp operation

Данная команда используется для того, чтобы отобразить эксплуатационные данные для DHCPv6-сервера.

show ipv6 dhcp operation

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить эксплуатационные данные для DHCPv6-сервера.

Пример

В данном примере показано, как отобразить эксплуатационные данные для DHCPv6-сервера.

```
switch# show ipv6 dhcp operation

DHCPv6 pool: pool1
  Prefix delegation pool: abc, prefix is 3000::/32 48
  Static bindings:
    Binding for client 00030001aabbcd000080
      IA PD: IA ID 0x0001
      Prefix: 3000:0:300::/48
      preferred lifetime 604800, valid lifetime 2592000
    preferred lifetime 604800, valid lifetime 2592000
    DNS server: 2345::2
    Domain name: pool1.com

DHCPv6 pool: test
  Address prefix: 1234::/64
  Static bindings:
    Binding for client 00030001aabbcd001234
      IA NA: IA ID not specified
      Address: 1234::1234
      preferred lifetime 604800, valid lifetime 2592000
    preferred lifetime 200, valid lifetime 300
    DNS server: 2000::2
    Domain name: test.com

switch#
```

27. Команды Digital Diagnostics Monitoring (DDM)

27-1 show interfaces transceiver

Данная команда используется для отображения текущих операционных параметров модуля SFP/SFP+.

```
show interfaces [INTERFACE-ID [, | -] transceiver [detail]
```

Параметры

<i>INTERFACE-ID</i>	(Опционально) Укажите интерфейсы, для которых необходимо отобразить статус Transceiver Monitoring. Если interface ID не указаны, будут отображены статусы Transceiver Monitoring для всех действующих интерфейсов.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
detail	(Опционально) Укажите, чтобы отобразить более подробную информацию.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить текущие операционные параметры Transceiver Monitoring для модуля SFP/SFP+ на указанных портах.

Пример

В данном примере показано, как отобразить текущие операционные параметры для всех портов, поддерживающих функцию Transceiver Monitoring.

```
Switch#show interfaces transceiver

++ : high alarm, + : high warning, - : low warning, -- : low alarm
mA: milliamperes, mW: milliwatts

Transceiver Monitoring traps: None

port      Temperature Voltage      Bias Current TX Power      RX Power
(Celsius) (V)          (mA)         (mW/dbm)     (mW/dbm)
-----
eth1/0/21 30.845      3.284        7.895        0.604        0.470
                    -2.189      -3.279

Total Entries: 1

Switch#
```

В данном примере показано, как отобразить подробную информацию Transceiver Monitoring для всех портов, поддерживающих данную функцию.

```
Switch#show interfaces transceiver detail

++ : high alarm, + : high warning, - : low warning, -- : low alarm
mA: milliamperes, mW: milliwatts
A: The threshold is administratively configured.

eth1/0/21
Transceiver Monitoring is enabled
Transceiver Monitoring shutdown action: None

Current      High-Alarm  High-Warning Low-Warning  Low-Alarm
Temperature(C) 30.803      78.000      73.000      -8.000      -13.000
Voltage(V)      3.284       3.700       3.600       3.000       2.900
Bias Current(mA) 7.890       11.800      10.800      5.000       4.000
TX Power(mW)    0.604       0.832       0.661       0.316       0.251
(dbm)           -2.191      -0.800      -1.800      -5.000      -6.000
RX Power(mW)    0.470       1.000       0.794       0.016       0.010
(dbm)           -3.283      0.000       -1.000      -18.013     -20.000

Switch#
```

27-2 snmp-server enable traps transceiver-monitoring

Данная команда используется для того, чтобы включить отправку всех или определенных SNMP-уведомлений Optical Transceiver Monitoring. Используйте форму **no**, чтобы отключить отправку уведомлений.

```
snmp-server enable traps transceiver-monitoring [alarm] [warning]
no snmp-server enable traps transceiver-monitoring [alarm] [warning]
```

Параметры

alarm	(Опционально) Укажите, чтобы включить/отключить отправку уведомлений уровня alarm (тревога).
--------------	--

warning	(Опционально) Укажите, чтобы включить/отключить отправку уведомлений уровня warning (предупреждение).
----------------	---

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если не указаны дополнительные параметры, будут включены/отключены все SNMP-уведомления Transceiver Monitoring.

Пример

В данном примере показано, как включить отправку уведомлений уровня warning.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps transceiver-monitoring warning
Switch(config)#
```

27-2 transceiver-monitoring action shutdown

Используйте данную команду, чтобы отключить порт при обнаружении события alarm (тревога) или warning (предупреждение). Используйте форму **no**, чтобы отключить данную функцию.

transceiver-monitoring action shutdown {alarm | warning}
no transceiver-monitoring action shutdown

Параметры

alarm	Укажите, чтобы отключить порт при обнаружении события alarm.
warning	Укажите, чтобы отключить порт при обнаружении события warning.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить интерфейс физического порта.

Данная команда позволяет указать, будет ли отключаться порт при обнаружении события alarm / события warning. Если функция Monitoring включена, отслеживаются события alarm и события warning. Событие alarm происходит, если отслеживаемые параметры выходят за пределы верхнего или нижнего порога alarm. Событие warning происходит, если отслеживаемые параметры выходят за пределы верхнего или нижнего порога warning.

Отключение порта контролируется модулем Error Disable без таймера Recover. Пользователь может включить порт вручную, применив команду **shutdown**, а затем команду **no shutdown**.

Пример

В данном примере показано, как настроить отключение порта Ethernet 1/0/1 при обнаружении события alarm.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# transceiver-monitoring action shutdown alarm
Switch(config-if)#
```

27-4 transceiver-monitoring bias-current

Данная команда используется для настройки порогов тока смещения на указанном порту. Используйте форму **no**, чтобы удалить заданные настройки.

```
transceiver-monitoring bias-current INTERFACE-ID {high | low} {alarm | warning} VALUE
no transceiver-monitoring bias-current INTERFACE-ID {high | low} {alarm | warning}
```

Параметры

<i>INTERFACE-ID</i>	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.
low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
<i>VALUE</i>	Укажите порог в диапазоне от 0 до 131 мА.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данный функционал доступен только для интерфейсов портов SFP+ с оптическими модулями, поддерживающими функцию Transceiver Monitoring.

Данная команда позволяет настроить пороги тока смещения на указанных портах. Заданные значения сохраняются как в системе, так и в трансиверах SFP/SFP+, а также будут направлены в модуль SFP/SFP+ в 16-битном формате.

Если конфигурируемый модуль SFP/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен в системе и отображен. При отсутствии пороговых значений, заданных пользователем, будут отображены значения, заданные производителем.

При помощи формы **no** данной команды можно удалить заданные пороговые значения, сохраненные в системе. При этом пороговые значения, сохраненные в трансиверах SFP/SFP+, остаются неизменными. Используйте форму **no**, чтобы предотвратить изменения пороговых значений в трансивере SFP/SFP+ при его первом подключении.

Пример

В данном примере показано, как настроить верхний порог warning для тока смещения на порту Ethernet 1/0/21. Указанное значение – 10,237 мА.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring bias-current ethernet 1/0/21 high warning 10.237

WARNING: A closest value 10.236 is chosen according to the transceiver-monitoring precision
definition

Switch(config)#
```

27-5 transceiver-monitoring enable

Данная команда используется для включения функции Optical Transceiver Monitoring на порту SFP+. Используйте форму **no**, чтобы отключить функцию Optical Transceiver Monitoring.

transceiver-monitoring enable
no transceiver-monitoring enable

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить интерфейс физического порта.

Данная команда позволяет включить/отключить функцию Optical Transceiver Monitoring на порту SFP+. Если функция Monitoring включена, отслеживаются события alarm и события warning. Событие alarm происходит, если отслеживаемые параметры выходят за пределы верхнего или нижнего порога alarm. Событие warning происходит, если отслеживаемые параметры выходят за пределы верхнего или нижнего порога warning.

Если трансивер SFP/SFP+ с функцией transceiver monitoring подключен к порту, на котором данная функция отключена, система не сможет определить аварийный статус трансивера SFP/SFP+, однако пользователь может проверить статус при помощи команды interface transceiver.

Пример

В данном примере показано, как включить функцию Transceiver Monitoring на порту Ethernet 1/0/21.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/21
Switch(config-if)# transceiver-monitoring enable
Switch(config-if)#
```

27-6 transceiver-monitoring rx-power

Данная команда используется для настройки порогов входной мощности на указанном порту. Используйте форму **no**, чтобы удалить заданные настройки.

```
transceiver-monitoring rx-power INTERFACE-ID {high | low} {alarm | warning} {mwatt VALUE | dbm
VALUE}
no transceiver-monitoring rx-power INTERFACE-ID {high | low} {alarm | warning}
```

Параметры

<i>INTERFACE-ID</i>	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.
low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
mwatt <i>VALUE</i>	Укажите порог входной мощности в диапазоне от 0 до 6,5535 мВт.
dbm <i>VALUE</i>	Укажите порог входной мощности в диапазоне от -40 до 8,1647 дБм.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данный функционал доступен только для интерфейсов портов SFP+ с оптическими модулями, поддерживающими функцию Transceiver Monitoring.

Данная команда позволяет настроить пороги входной мощности на указанном порту. Заданные значения сохраняются как в системе, так и в трансиверах SFP/SFP+, а также будут направлены в модуль SFP/SFP+ в 16-битном формате.

Если конфигурируемый модуль SFP/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен в системе и отображен. При отсутствии пороговых значений, заданных пользователем, будут отображены значения, заданные производителем.

При помощи формы **no** данной команды можно удалить заданные пороговые значения, сохраненные в системе. При этом пороговые значения, сохраненные в трансиверах SFP/SFP+, остаются неизменными. Используйте форму **no**, чтобы предотвратить изменения пороговых значений в трансивере SFP/SFP+ при его первом подключении.

Пример

В данном примере показано, как настроить нижний порог warning для входной мощности на порту Ethernet 1/0/21. Указанное значение – 0,135 мВт.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring rx-power ethernet 1/0/21 low warning mwatt 0.135
Switch(config)#
```

27-7 transceiver-monitoring temperature

Данная команда используется для настройки порогов температуры на указанном порту. Используйте форму **no**, чтобы удалить заданные настройки.

transceiver-monitoring temperature *INTERFACE-ID* {**high** | **low**} {**alarm** | **warning**} *VALUE*
no transceiver-monitoring temperature *INTERFACE-ID* {**high** | **low**} {**alarm** | **warning**}

Параметры

<i>INTERFACE-ID</i>	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.
low	Укажите нижний порог. Значения ниже заданного порога

	свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
VALUE	Укажите порог температуры в диапазоне от -128 до +127,996 °C.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данный функционал доступен только для интерфейсов портов SFP+ с оптическими модулями, поддерживающими функцию Transceiver Monitoring.

Данная команда позволяет настроить пороги температуры на указанном порту. Заданные значения сохраняются как в системе, так и в трансиверах SFP/SFP+, а также будут направлены в модуль SFP/SFP+ в 16-битном формате.

Если конфигурируемый модуль SFP/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен в системе и отображен. При отсутствии пороговых значений, заданных пользователем, будут отображены значения, заданные производителем.

При помощи формы по данной команды можно удалить заданные пороговые значения, сохраненные в системе, при этом пороговые значения, сохраненные в трансиверах SFP/SFP+, остаются неизменными. Используйте форму `no`, чтобы предотвратить изменения пороговых значений в трансивере SFP/SFP+ при его первом подключении.

Пример

В данном примере показано, как настроить верхний порог alarm для температуры на порту Ethernet 1/0/21. Указанное значение – 127,994 °C.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring temperature ethernet 1/0/21 high alarm 127.994

WARNING: A closer value of 127.992 is chosen according to the transceiver-monitoring precision
definition

Switch(config)#
```

27-8 transceiver-monitoring tx-power

Данная команда используется для настройки порогов выходной мощности на указанном порту. Используйте форму `no`, чтобы удалить заданные настройки.

```

transceiver-monitoring tx-power INTERFACE-ID {high | low} {alarm | warning} {mwatt VALUE |dbm
VALUE}
no transceiver-monitoring tx-power INTERFACE-ID {high | low} {alarm | warning}

```

Параметры

<i>INTERFACE-ID</i>	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.
low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
mwatt VALUE	Укажите порог выходной мощности в диапазоне от 0 до 6,5535 мВт.
dbm VALUE	Укажите порог выходной мощности в диапазоне от -40 до 8,1647 дБм.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данный функционал доступен только для интерфейсов портов SFP+ с оптическими модулями, поддерживающими функцию Transceiver Monitoring.

Данная команда позволяет настроить пороги выходной мощности на указанных портах. Заданные значения сохраняются как в системе, так и в трансиверах SFP/SFP+, а также будут направлены в модуль SFP/SFP+ в 16-битном формате.

Если конфигурируемый модуль SFP/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен в системе и отображен. При отсутствии пороговых значений, заданных пользователем, будут отображены значения, заданные производителем.

При помощи формы **no** данной команды можно удалить заданные пороговые значения, сохраненные в системе. При этом предельные значения, сохраненные в трансиверах SFP/SFP+, остаются неизменными. Используйте форму **no**, чтобы предотвратить изменения пороговых значений в трансивере SFP/SFP+ при его первом подключении.

Пример

В данном примере показано, как настроить нижний порог warning для выходной мощности на порту Ethernet 1/0/21. Указанное значение – 0,181 мВт.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring tx-power ethernet 1/0/21 low warning mwatt 0.181
Switch(config)#
```

27-9 transceiver-monitoring voltage

Данная команда используется для настройки порогов напряжения на указанном порту. Используйте форму **no**, чтобы удалить заданные настройки.

transceiver-monitoring voltage *INTERFACE-ID* {**high** | **low**} {**alarm** | **warning**} *VALUE*
no transceiver-monitoring voltage *INTERFACE-ID* {**high** | **low**} {**alarm** | **warning**}

Параметры

<i>INTERFACE-ID</i>	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.
low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
<i>VALUE</i>	Укажите порог напряжения в диапазоне от 0 до 6,5535 В.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данный функционал доступен только для интерфейсов портов SFP+ с оптическими модулями, поддерживающими функцию Transceiver Monitoring.

Данная команда позволяет настроить пороги напряжения на указанных портах. Заданные значения сохраняются как в системе, так и в трансиверах SFP/SFP+, а также будут направлены в модуль SFP/SFP+ в 16-битном формате.

Если конфигурируемый модуль SFP/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен в системе и отображен. При отсутствии пороговых значений, заданных пользователем, будут отображены значения, заданные производителем.

При помощи формы **no** данной команды можно удалить заданные пороговые значения, сохраненные в системе. При этом пороговые значения, сохраненные в трансиверах SFP/SFP+, остаются неизменными.

Используйте форму **no**, чтобы предотвратить изменения предельных значений в трансивере SFP/SFP+ при его первом подключении.

Пример

В данном примере показано, как настроить нижний порог alarm для напряжения на порту ethernet 1/0/21. Указанное значение – 0,005 В.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring voltage ethernet 1/0/21 low alarm 0.005
Switch(config)#
```

28. Команды клиента D-Link Discovery Protocol (DDP)

28-1 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 глобально, но включена на всех физических портах.

Режим ввода команды

Global Configuration Mode Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить/отключить функцию клиента DDP глобально или на физическом порту.

Если на порту отключена функция DDP, данный порт не будет ни обрабатывать, ни генерировать DDP-сообщения. Полученные портом DDP-сообщения распространяются в рамках широковещательного домена.

Пример

В данном примере показано, как включить DDP глобально.

```
Switch# configure terminal
Switch(config)# ddp
Switch(config)#
```

В данном примере показано, как включить DDP на порту 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ddp
Switch(config-if)#
```

28-2 ddp report-timer

Данная команда используется для настройки интервала между двумя последовательными сообщениями DDP Report. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ddp report-timer {30 | 60 | 90 | 120 | Never}
no ddp report-timer
```

Параметры

30	Укажите, чтобы установить интервал 30 секунд.
60	Укажите, чтобы установить интервал 60 секунд.
90	Укажите, чтобы установить интервал 90 секунд.
120	Укажите, чтобы установить интервал 120 секунд.
Never	Укажите, чтобы не отправлять сообщения Report.

По умолчанию

Параметр по умолчанию – **Never**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить интервал между двумя последовательными сообщениями DDP Report.

Пример

В данном примере показано, как установить интервал 60 секунд.

```
Switch# configure terminal
Switch(config)# ddp report-timer 60
Switch(config)#
```

28-3 show ddp

Данная команда используется для отображения настроек DDP на коммутаторе.

```
show ddp [interfaces {INTERFACE-ID [, | -]}]
```

Параметры

<i>INTERFACE-ID</i>	Укажите interface ID.
---------------------	-----------------------

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию о DDP на коммутаторе.

Пример

В данном примере показано, как отобразить общую информацию о DDP.

```
Switch#show ddp

D-Link Discovery Protocol state: Enabled
Report timer: 30 seconds

Switch#
```

В данном примере показано, как отобразить информацию о DDP на порту 1/0/1.

```
Switch#show ddp interface ethernet 1/0/1

Interface      State
-----
eth1/0/1      Enabled

Switch#
```


29. Команды D-Link Unidirectional Link Detection (DULD)

29-1 duld enable

Данная команда используется для включения функции Ethernet OAM Unidirectional Link Detection (обнаружение потери связи в одном направлении) на указанном порту. Используйте форму **no**, чтобы отключить данную функцию.

duld enable
no duld enable

Параметры

Нет

По умолчанию

По умолчанию функция DULD отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

D-Link Unidirectional Link Detection представляет собой расширение для 802.3ah Ethernet OAM. Оно позволяет обнаружить однонаправленный Ethernet-канал типа «точка-точка» без поддержки PDU. Для обнаружения используются сообщения OAM, указанные vendor-ом. Процесс обнаружения начинается после запуска обнаружения OAM, но не завершается в установленное время обнаружения Discovery Time.

Пример

В данном примере показано, как включить, а затем отключить Ethernet OAM Unidirectional Link Detection на интерфейсе 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# duld enable
Switch(config-if)# no duld enable
Switch(config-if)#
```

29-2 duld action

Данная команда используется для настройки функции Ethernet OAM Unidirectional Link Detection (обнаружение потери связи в одном направлении) на указанном порту. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

duld action shutdown
no duld action

Параметры

Нет

По умолчанию

По умолчанию опция Shutdown выключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить функцию Ethernet OAM Unidirectional Link Detection на указанном порту.

Пример

В данном примере показано, как включить опцию Shutdown в режиме OAM DULD на интерфейсе 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# duld action shutdown
Switch(config-if)#
```

29-3 duld discovery-time

Данная команда используется для настройки Discovery Time (время обнаружения) функции Ethernet OAM Unidirectional Link Detection (обнаружение потери связи в одном направлении). Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

duld discovery-time SECONDS
no duld discovery-time

Параметры

<i>SECONDS</i>	Укажите значение Discovery Time в диапазоне от 5 до 65535 секунд.
----------------	---

По умолчанию

Значение по умолчанию – 5 секунд.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если обнаружение OAM не было успешно завершено до момента истечения установленного значения Discovery Time, будет запущена функция OAM Unidirectional Link Detection.

Пример

В данном примере показано, как настроить значение DULD Discovery Time на интерфейсе 1/0/1. Установленное значение – 7 секунд.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# duld discovery-time 7
Switch(config-if)#
```

29-4 show duld

Данная команда используется для отображения информации об Ethernet OAM Unidirectional Link Detection (обнаружение потери связи в одном направлении).

show duld [interface *INTERFACE-ID* [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите, чтобы отобразить interface ID физического порта.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию о DULD.

Пример

В данном примере показано, как отобразить информацию об Ethernet OAM Unidirectional Link Detection на порту Ethernet 1/0/1.

```
Switch#show duld interface ethernet 1/0/1

Ethernet 1/0/1
  Admin State       : Enabled
  Oper Status       : Disabled
  Action            : Normal
  Link Status       : Unknown
  Discovery Time (Sec) : 7

Switch#
```

29-5 duld recovery-time

Данная команда используется для настройки Automatic Recovery Time (время автоматического восстановления) Ethernet OAM Unidirectional Link Detection (обнаружение потери связи в одном направлении). Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
duld recovery-time {0 | SECONDS}
no duld recovery-time
```

Параметры

<i>SECONDS</i>	Укажите значение Automatic Recovery Time в диапазоне от 60 до 1000000 секунд. 0 означает, что функция отключена.
----------------	--

По умолчанию

Значение по умолчанию – 60 секунд.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы установить время, используемое механизмом auto-recovery для проверки на наличие Unidirectional Link. После истечения таймера порт, отключенный при помощи DULD, будет восстановлен автоматически.

Пример

В данном примере показано, как настроить значение DULD Recovery Time. Установленное значение – 120 секунд.

```
Switch#configure terminal
Switch(config)#duld recovery-time 120
Switch(config)#
```

30. Команды Domain Name System (DNS)

30-1 clear host

Данная команда используется для удаления динамически изученных записей узла в режиме Privileged User Mode.

```
clear host {all} [HOST-NAME]
```

Параметры

all	Укажите, чтобы удалить все записи узла.
<i>HOST-NAME</i>	(Опционально) Укажите, чтобы удалить указанную динамически изученную запись узла.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы удалить запись узла или все записи узла, которые динамически изучены DNS Resolver или Caching Server.

Пример

В данном примере показано, как удалить динамически изученную запись «www.abc.com» из таблицы узлов.

```
Switch# clear host www.abc.com
Switch#
```

30-2 ip dns server

Данная команда используется для включения функции DNS Caching Name Server. Используйте форму **no**, чтобы отключить данную функцию.

```
ip dns server
no ip dns server
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Система поддерживает функцию DNS Caching Name Server. Если данная функция и IP Domain-Lookup включены, система направляет пакет запроса DNS 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 DNS Caching Name Server.

```
Switch# configure terminal
Switch(config)# ip dns server
Switch(config)#
```

30-3 ip dns lookup

Данная команда используется для включения DNS-поиска динамических кэшированных или статических созданных записей узла. Используйте форму **no**, чтобы отключить DNS-поиск динамических или статических записей узла.

```
ip dns lookup [static] [cache]
no ip dns lookup [static] [cache]
```

Параметры

static	(Опционально) Укажите, чтобы включить/отключить поиск статических записей перед отправкой запроса на Name Server.
cache	(Опционально) Укажите, чтобы включить/отключить поиск динамического кэша перед отправкой запроса на Name Server.

По умолчанию

Параметры по умолчанию – **static** и **cache**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

В процессе поиска имени домена по умолчанию сначала будет проведена проверка статического и динамического кэша, а затем, если не найдены соответствующие записи, будет отправлен запрос на Name Server. Используйте данную команду, чтобы отключить опцию поиска статических/динамических записей кэша до момента отправки запросов на Name Server. При использовании команды без указания дополнительных параметров, параметры **static** и **cache** включаются/отключаются одновременно.

Пример

В данном примере показано, как включить поиск статического узла для ответа на запрос.

```
Switch# configure terminal
Switch(config)# ip dns lookup static
Switch(config)#
```

30-4 ip domain lookup

Данная команда используется для включения DNS, что позволяет использовать функцию Domain Name Resolution. Используйте форму **no**, чтобы отключить данную функцию.

ip domain lookup
no ip domain lookup

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду **ip domain lookup**, чтобы включить функцию Domain Name Resolution. DNS Resolver отправляет запрос на указанный Name Server. Ответ, отсылаемый Name Server, будет кэширован и использован для ответа на последующие запросы.

Пример

В данном примере показано, как включить функцию Domain Name Resolution.

```
Switch# configure terminal
Switch(config)# ip domain lookup
Switch(config)#
```

30-5 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Имя узла, указанное в этой команде, должно быть подходящим. Чтобы удалить статическую запись узла, используйте форму по 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)#
```

30-6 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 несколько IP-адресов, разделяя их при помощи пробелов. Можно указать не более 2 серверов.
<i>IPV6-ADDRESS2</i>	Укажите несколько IPv6-адресов, разделяя их при помощи пробелов. Можно указать не более 2 серверов.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы сконфигурировать DNS-сервер. Если система не может получить ответ от DNS-сервера, будет отправлен запрос на следующий сервер, и так до тех пор, пока ответ не будет получен. Если Name Servers уже сконфигурированы, то серверы, сконфигурированные позже, будут добавлены в список серверов. Можно сконфигурировать до 4 Name Servers.

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)#
```

30-7 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 указанного Name Server. Доступный диапазон значений: от 1
----------------	---

до 60 секунд.

По умолчанию

Значение по умолчанию – 3 секунды.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить максимальное значение времени ожидания ответа от указанного Name Server.

Пример

В данном примере показано, как указать значение тайм-аута 5 секунд.

```
Switch# configure terminal
Switch(config)# ip name-server timeout 5
Switch(config)#
```

30-8 show hosts

Данная команда используется для отображения настроек DNS.

show hosts

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию о настройках DNS.

Пример

В данном примере показано, как отобразить информацию о настройках DNS.

```
Switch#show hosts

Number of Static Entries:  3
Number of Dynamic Entries: 0

Host Name:      www.abc.com
IP Address:     192.168.5.243
Age:           forever

Host Name:      www.yes.com
IP Address:     10.0.0.88
Age:           forever

Host Name:      www.yes.com
IPv6 Address:   2001:1::1
Age:           forever

Switch#
```

30-9 show ip name-server

Данная команда используется для отображения текущих DNS.

```
show ip name-server
```

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить DNS.

Пример

В данном примере показано, как отобразить DNS.

```
Switch#show ip name-server  
  
Name servers are: 192.168.5.134  
Name servers are: 5001:5::2  
  
Switch#
```

31. Команды предотвращения атак DoS

31-1 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения и настройки механизма предотвращения атак DoS для определенного типа атак DoS или для всех поддерживаемых типов. Механизмы предотвращения атак DoS (сопоставление и принятие мер) являются функциями аппаратного обеспечения.

При включенном предотвращении атак DoS коммутатор сохранит событие (лог) в журнале, если был получен хотя бы один «атакующий» пакет.

Команда **no dos-prevention** с ключевым словом **all** используется для отключения механизма предотвращения атак DoS для всех поддерживаемых типов. Все настройки будут возвращены к значениям по умолчанию для определенных типов атак.

Следующие распространенные типы DoS-атак могут быть обнаружены большинством коммутаторов:

- **Blat:** данный тип атаки включает в себя отправку устройству пакетов с портом источника TCP/UDP, равным порту назначения. Это может послужить причиной того, что устройство будет отвечать самому себе.
- **Land:** атака LAND включает в себя отправку устройству IP-пакетов с адресом источника и назначения, равным адресу устройства. Это может послужить причиной того, что устройство будет непрерывно отвечать самому себе.
- **TCP-NULl-scan:** сканирование порта с использованием определенных пакетов, содержащих последовательность чисел от 0 и не содержащих флаги.
- **TCP-SYN-fin:** сканирование порта с использованием определенных пакетов, содержащих флаги SYN и FIN.

- **TCP-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.



Примечание: некоторые функции, использующие протокол NTP, могут работать некорректно, если включено предотвращение DoS-атак типа Blat, так как они используют один и тот же номер порта.

Пример

В данном примере показано, как включить механизм предотвращения атак DoS для атаки Land.

```
Switch# configure terminal
Switch(config)# dos-prevention land
Switch(config)#
```

В данном примере показано, как включить механизм предотвращения атак DoS для атак всех поддерживаемых типов.

```
Switch# configure terminal
Switch(config)# dos-prevention all
Switch(config)#
```

В данном примере показано, как отключить механизм предотвращения атак DoS для атак всех поддерживаемых типов.

```
Switch# configure terminal
Switch(config)# no dos-prevention all
Switch(config)#
```

31-2 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

User-Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для получения информации о статусе предотвращения атак DoS.

Пример

В данном примере 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#
```

31-3 snmp-server enable traps dos-prevention

Данная команда используется для отправки SNMP-уведомлений о DoS-атаках. Для отключения данной команды используйте форму **no**.

snmp-server enable traps dos-prevention

no snmp-server enable traps dos-prevention

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если предотвращение атак DoS включено, каждые пять минут коммутатор будет записывать в журнал событие, если какой-либо атакующий пакет будет принят за этот промежуток времени. Используйте данную команду, чтобы включить или отключить отправку уведомлений SNMP для таких событий.

Пример

В данном примере показано, как включить отправку трапов для атак DoS.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps dos-prevention
Switch(config)#
```

32. Команды Dynamic ARP Inspection

32-1 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Имя должно быть уникальным среди всех списков доступа. Имя чувствительно к регистру. В конце списка доступа указан запрет в доступе всем, кого нет в списке разрешений.

Пример

В данном примере показано, как настроить список доступа ARP с двумя разрешающими записями.

```
Switch# configure terminal
Switch(config)# arp access-list static-arp-list
Switch(config-arp-nacl)# permit ip 10.20.0.0 0.0.255.255 mac any
Switch(config-arp-nacl)# permit ip 10.30.0.0 0.0.255.255 mac any
Switch(config-arp-nacl)#
```

32-2 clear ip arp inspection log

Данная команда используется для очистки буфера журнала ARP Inspection.

```
clear ip arp inspection log
```

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для очистки буфера журнала ARP Inspection.

Пример

В данном примере показано, как очистить журнал ARP Inspection.

```
Switch# clear ip arp inspection log
Switch#
```

32-3 clear ip arp inspection statistics

Данная команда используется для удаления данных статистики Dynamic ARP Inspection.

clear ip arp inspection statistics {all | vlan VLAN-ID [, | -]}

Параметры

all	Укажите для удаления данных статистики Dynamic ARP Inspection для всех VLAN.
vlan VLAN-ID	Укажите VLAN или диапазон VLAN.
,	(Опционально) Выделение серии VLAN или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Выделение диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для удаления данных статистики Dynamic ARP Inspection.

Пример

В данном примере показано, как удалить данные статистики Dynamic ARP Inspection для VLAN 1.

```
Switch# clear ip arp inspection statistics vlan 1
Switch#
```

32-4 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.
vlan <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.
static	(Опционально) Укажите при необходимости отбрасывать пакет, если пара привязки IP-to-Ethernet MAC не разрешена ARP ACL.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для указания списка доступа ARP, который будет использоваться для проверки ARP Inspection для VLAN. Для одной VLAN можно указать один список доступа.

Dynamic ARP Inspection проверяет ARP-пакеты, полученные в VLAN, для проверки корректности пары привязки IP-адреса источника и MAC-адреса источника. Во время проверки произойдет сопоставление адреса привязки и записей из таблицы привязки DHCP Snooping. Проверка будет производиться, если данная команда сконфигурирована.

Списки управления доступом ARP (ARP ACL) имеют более высокий приоритет над таблицей привязки DHCP Snooping. Если пакету явно запрещен доступ списком управления доступа, пакет будет отброшен. Если пакету неявно запрещен доступ, он будет дополнительно сопоставлен с записями привязки DHCP Snooping, если не указано ключевое слово «static». Если пакету неявно запрещен доступ и указано ключевое слово «static», пакет будет отброшен.

Пример

В данном примере показано, как применить список управления доступом ARP (ARP ACL) static ARP list в VLAN 10 для DAI.

```
Switch# configure terminal
Switch(config)# ip arp inspection filter static-arp-list vlan 10
Switch(config)#
```

32-5 ip arp inspection limit

Данная команда используется для ограничения скорости входящих ARP-запросов и ответов на интерфейсе. При использовании формы **no** команда вернется к значениям по умолчанию.

ip arp inspection limit {rate VALUE [burst interval SECONDS] | none}
no ip arp inspection limit

Параметры

rate VALUE	Укажите максимальное количество ARP-пакетов в секунду, которое может быть обработано. Доступен диапазон значений от 1 до 150.
burst interval SECONDS	(Опционально) Укажите разрешенную величину продолжительности всплеска (burst duration) ARP-пакетов. Доступен диапазон значений от 1 до 15. Если не указано, значение по умолчанию составляет 1 секунду.
none	Укажите, чтобы скорость передачи ARP-пакетов не была ограничена.

По умолчанию

Для недоверенных интерфейсов DAI ограничение скорости составляет 15 пакетов в секунду синтервалом всплеска burst interval в 1 секунду.

Для доверенных интерфейсов DAI ограничений нет.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется и для доверенных, и для недоверенных интерфейсов. Если скорость ARP-пакетов в секунду превышает ограничение и условия для настроенной продолжительности всплеска (burst duration), порт автоматически отключится из-за ошибки.

Пример

В данном примере показано, как назначить ограничение скорости входящих ARP-запросов до 30 пакетов в секунду и интервал проверки интерфейса до 5 следующих секунд.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/10
Switch(config-if)# ip arp inspection limit rate 30 burst interval 5
Switch(config-if)#
```

32-6 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки максимального количества записей в буфере журнала. Буфер журнала ARP Inspection хранит информацию об ARP-пакетах. Первый пакет, прошедший через проверку, будет отправлен в модуль системного журнала (syslog) и записан в буфер журнала проверки. Последующие пакеты из той же сессии не будут отправлены в модуль журнала, если только его запись в буфере журнала не будет удалена. Если буфер журнала полон, но события продолжают поступать, они не будут записаны в журнал. Если пользователь задает размер буфера меньше текущего номера записи, буфер журнала (лога) будет очищен автоматически.

Пример

В данном примере показано, как изменить размер буфера на 64.

```
Switch# configure terminal
Switch(config)# ip arp inspection log-buffer entries 64
Switch(config)#
```

32-7 ip arp inspection trust

Данная команда используется для назначения доверенного интерфейса для Dynamic ARP Inspection. При использовании формы **no** команда отключит режим доверенного интерфейса.

```
ip arp inspection trust
no ip arp inspection trust
```

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если интерфейс находится в состоянии Trust (доверенный), ARP-пакеты, поступающие на интерфейс, не будут проверяться. Если интерфейс находится в состоянии Untrusted (недоверенный), ARP-пакеты, поступающие на порт и принадлежащие VLAN, в которой включена проверка, будут проверяться.

Пример

В данном примере показано, как настроить состояние Trust (доверенный) для порта 1/0/3 для DAI.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ip arp inspection trust
Switch(config-if)#
```

32-8 ip arp inspection validate

Данная команда используется для указания дополнительных проверок при ARP Inspection. При использовании формы **no** команда отключит дополнительные проверки.

```
ip arp inspection validate [src-mac] [dst-mac] [ip]
no ip arp inspection validate [src-mac] [dst-mac] [ip]
```

Параметры

src-mac	(Опционально) Укажите для проверки пакетов ARP-запросов и ответов, а также согласованности MAC-адреса источника в заголовке Ethernet с MAC-адресом источника в ARP заголовке.
dst-mac	(Опционально) Укажите для проверки пакетов ARP-ответов, а также согласованности MAC-адреса источника в заголовке Ethernet с MAC-адресом источника в ARP заголовке.
ip	(Опционально) Укажите для проверки содержимого ARP на наличие недопустимых и непредвиденных IP-адресов. Укажите для проверки допустимости IP-адреса в заголовке ARP. Проверяются IP-адреса источника во всех ARP-запросах и ответах, а также IP-адрес назначения в ARP-ответе. Пакеты, отправляемые на IP-адреса 0.0.0.0, 255.255.255.255 и все IP-адреса многоадресной рассылки, отбрасываются. IP-адреса источника проверяются во всех ARP-запросах и ответах, а IP-адреса назначения проверяются только в ARP-ответах.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для указания дополнительных проверок во время Dynamic ARP Inspection. Указанные проверки будут производиться с пакетами, присылаемыми с недоверенных интерфейсов и принадлежащих VLAN, для которых включена IP ARP Inspection. Если никакие параметры не указаны, все опции включены или выключены. При использовании формы по 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)#
```

32-9 ip arp inspection vlan

Данная команда используется для включения Dynamic ARP Inspection для определенных VLAN. При использовании формы **no** команда отключит Dynamic ARP Inspection для VLAN.

ip arp inspection vlan *VLAN-ID* [, | -]

no ip arp inspection vlan VLAN-ID [, | -]**Параметры**

vlan VLAN-ID	Укажите VLAN, для которой необходимо включить или отключить функцию ARPInspection.
,	(Опционально) Выделение серии или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию ARP Inspection отключена для всех VLAN.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если VLAN включена для ARP Inspection, проверяться будут ARP-пакеты, включая пакеты ARP- запроса и ответа, принадлежащие VLAN и отправленные на недоверенный интерфейс. Если пара привязки IP-to-MAC MAC-адреса источника и IP-адреса источника не разрешены ARP ACL, либо таблицей привязки DHCP Snooping, ARP-пакеты будут отброшены. Помимо проверки привязки адреса, осуществляться будет дополнительная проверка, определяемая командой **ip arp inspection validate**.

Пример

В данном примере показано, как включить ARP Inspection в VLAN 2.

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 2
Switch(config)#
```

32-10 ip arp inspection vlan logging

Данная команда используется для управления типом пакетов, которые будут регистрироваться (логироваться). При использовании формы **no** команда вернется к значениям по умолчанию.

```
ip arp inspection vlan VLAN-ID [, | -] logging {acl-match {permit | all | none} | dhcp-bindings {permit | all | none}}
no ip arp inspection vlan VLAN-ID [, | -] logging {acl-match | dhcp-bindings}
```

Параметры

VLAN-ID	Укажите VLAN, для которой необходимо включить или отключить функцию управления логированием.
----------------	--

,	(Опционально) Выделение серии или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон VLAN. Пробелы до и после дефиса недопустимы.
acl-match	Укажите критерии логирования для пакетов, отброшенных или разрешенных на основе совпадения со списком управления доступом (ACL).
permit	Укажите для логирования, разрешенного сконфигурированным списком управления доступом (ACL).
all	Укажите для логирования, разрешенного или запрещенного сконфигурированным списком управления доступом (ACL).
none	Укажите, чтобы отменить логирование пакетов на основе совпадения со списком управления доступом (ACL).
dhcp-bindings	Укажите критерии логирования для пакетов, отброшенных или разрешенных на основе совпадения с привязкой DHCP.
permit	Укажите для логирования, разрешенного привязкой DHCP.
all	Укажите для логирования, разрешенного или запрещенного привязкой DHCP.
none	Укажите, чтобы отменить логирование всех пакетов, разрешенных или запрещенных на основе привязки DHCP.

По умолчанию

Все запрещенные и отброшенные пакеты логируются.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте форму **no**, чтобы команда вернулась к критериям логирования по умолчанию.

Пример

В данном примере показано, как настроить ARP Inspection во VLAN 1 для добавления пакетов в журнал на основе списка управления доступом (ACL).

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 1 logging acl-match all
Switch(config)#
```

32-11 permit | deny (arp access-list)

Данная команда используется для управления доступом ARP-записи. Используйте команду **deny** для создания запрещающей ARP-записи. При использовании формы **no** команда удалит запись.

{permit | deny} ip {any | host SENDER-IP | SENDER-IP SENDER-IP-MASK} mac {any | host SENDER-MAC | SENDER-MAC SENDER-MAC-MASK}
no {permit | deny} ip {any | host SENDER-IP | SENDER-IP SENDER-IP-MASK} mac {any | host SENDER-MAC | SENDER-MAC SENDER-MAC-MASK}

Параметры

ip	Укажите IP-адрес источника.
any	Укажите для сопоставления любого IP-адреса источника.
host SENDER-IP	Укажите для сопоставления единственного IP-адреса источника.
SENDER-IP SENDER-IP-MASK	Укажите для сопоставления группы IP-адресов источника с помощью битовой маски (bitmap). Проверяться будет бит, соответствующий значению бита 1. Формат ввода тот же, что и для IP-адреса.
mac	Укажите MAC-адрес.
any	Укажите для сопоставления любого MAC-адреса источника.
host SENDER-MAC	Укажите для сопоставления единственного MAC-адреса источника.
SENDER-MAC SENDER-MAC-MASK	Укажите для сопоставления группы MAC-адресов источника с помощью битовой маски (bitmap). Проверяться будет бит, соответствующий значению бита 1. Формат ввода тот же, что и для MAC-адреса.

По умолчанию

Нет

Режим ввода команды

ARP Access-list Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте опцию **permit any**, чтобы команда разрешила доступ остальным пакетам, не прошедшим проверку по предыдущим правилам.

Пример

В данном примере показано, как настроить список доступа ARP с двумя разрешенными записями.

```
Switch# configure terminal
Switch(config)# arp access-list static-arp-list
Switch(config-arp-nacl)# permit ip 10.20.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)# permit ip 10.30.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)#
```

32-12 show ip arp inspection

Данная команда используется для отображения статуса DAI для указанного диапазона VLAN.

show ip arp inspection [interface *INTERFACE-ID* [, | -]] statistics [vlan *VLAN-ID* [, | -]]

Параметры

interface <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.
statistics	(Опционально) Указывает данные статистики DAI.
vlan <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

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения статуса DAI для указанного диапазона VLAN.

Пример

В данном примере показано, как включить отображение параметров статистики пакетов, которые были обработаны DAI для VLAN 10.

```
Switch# show ip arp inspection statistics vlan 10

VLAN    Forwarded    Dropped    DHCP Drops    ACL Drops
-----
10      21546        145261     145261        0
VLAN    DHCP Permits  ACL Permits  Source MAC Failures
-----
10      21546         0           0
VLAN    Dest MAC Failures  IP Validation Failures
-----
10      0                0

Switch#
```

В данном примере показано, как включить отображение параметров статистики пакетов, которые были обработаны DAI для всех активных VLAN.

```
Switch# show ip arp inspection statistics

VLAN    Forwarded    Dropped    DHCP Drops    ACL Drops
-----
1       0            0           0             0
2       0            0           0             0
10      21546        145261     145261        0
100     0            0           0             0
200     0            0           0             0
1024    0            0           0             0
VLAN    DHCP Permits  ACL Permits  Source MAC Failures
-----
1       0            0           0
2       0            0           0
10      21546         0           0
100     0            0           0
200     0            0           0
1024    0            0           0
VLAN    Dest MAC Failures  IP Validation Failures
-----
1       0                0
2       0                0
10      0                0
100     0                0
200     0                0
1024    0                0

Switch#
```

Отображаемые параметры

VLAN	VLAN ID, на которой действует ARP Inspection.
Forwarded	Количество ARP-пакетов, переадресованных ARP Inspection.

Dropped	Количество ARP-пакетов, отброшенных ARP Inspection.
DHCP Drops	Количество ARP-пакетов, отброшенных таблицей DHCP Snooping.
ACL Drops	Количество ARP-пакетов, отброшенных с помощью ARP правил ACL (ARP ACL).
DHCP Permits	Количество ARP-пакетов, разрешенных таблицей привязки DHCP Snooping.
ACL Permits	Количество ARP-пакетов, разрешенных правилом ARP ACL.
Source MAC Failures	Количество ARP-пакетов, не прошедших проверку MAC-адреса источника.
Dest MAC Failures	Количество ARP-пакетов, не прошедших проверку MAC-адреса назначения.
IP Validation Failures	Количество ARP-пакетов, не прошедших проверку IP-адреса.

Пример

В данном примере показано, как включить отображение настроек и статус работы DAI.

```
Switch#show ip arp inspection

Source MAC Validation      : Enabled
Destination MAC Validation: Disabled
IP Address Validation      : Disabled
VLAN State      ACL Match      Static ACL
-----
10  Disabled static-arp-list      No
VLAN ACL Logging DHCP Logging
-----
10  Deny      Deny

Switch#
```

Отображаемые параметры

VLAN	VLAN ID, на которой действует ARP Inspection.
State	Состояние настроек ARP Inspection. Enabled: ARP Inspection работает. Disabled: ARP Inspection не работает.
ACL Match	Имя указанного списка управления доступом ARP (ARP ACL).
Static ACL	Настройки статического списка управления доступом (static ACL). Yes: статический список управления доступом (static ARP ACL) настроен. No: статический список управления доступом (static ARP ACL) не настроен.
ACL logging	Состояние логирования для пакетов, отброшенных или разрешенных на основесопадения 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.

Пример

В данном примере показано, как включить отображение состояния для Ethernet 1/0/10.

```
Switch#show ip arp inspection interfaces ethernet 1/0/10

Interface      Trust State Rate(pps) Burst Interval
-----
eth1/0/10      trusted  None      1
Total Entries: 1

Switch#
```

В данном примере показано, как включить отображение состояний для интерфейсов коммутатора.

```
Switch#show ip arp inspection interfaces

Interface      Trust State Rate(pps) Burst Interval
-----
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
eth1/0/8       untrusted  15         1
eth1/0/9       untrusted  15         1
eth1/0/10      trusted   None        1
eth1/0/11      untrusted  15         1
eth1/0/12      untrusted  15         1
eth1/0/13      untrusted  15         1
eth1/0/14      untrusted  15         1
eth1/0/15      untrusted  15         1
eth1/0/16      untrusted  15         1
eth1/0/17      untrusted  15         1
eth1/0/18      untrusted  15         1
eth1/0/19      untrusted  15         1
eth1/0/20      untrusted  15         1
eth1/0/21      untrusted  15         1

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Отображаемые параметры

Interface	Имя интерфейса, на котором работает ARP Inspection.
Trust State	Состояние интерфейса. trusted: данный интерфейс является доверенным портом ARP Inspection, все ARP-пакеты будут достоверны, и не будут проходить авторизацию. untrusted: данный интерфейс является недоверенным портом ARP Inspection, все ARP-пакеты будут проходить авторизацию.
Rate (pps)	Верхняя граница количества входящих пакетов, обрабатываемых в секунду.
Burst Interval	Последовательный интервал в секундах, в течение которого на интерфейсе анализируется частота появления ARP-трафика.

32-13 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 командыUser/Privileged EXEC Mode
Любой режим конфигурирования**Уровень команды по умолчанию**

Уровень 1

Использование команды

Данная команда используется для отображения содержимого буфера лога (журнала) ARP Inspection.

Пример

В данном примере показано, как включить отображение буфера лога (журнала) ARP Inspection.

```
Switch#show ip arp inspection log
Total log buffer size: 64

Interface      VLAN  Sender IP      Sender MAC      Occurrence
-----
eth1/0/1      100  10.20.1.1      00-20-30-40-50-60  1 (2013-12-28 23:08:66)
eth1/0/2      100  10.5.10.16     55-66-20-30-40-50  2 (2013-12-02 00:11:54)
eth1/0/3      100  10.58.2.30     10-22-33-44-50-60  1 (2013-12-30 12:01:38)

Total Entries: 3

Switch#
```

Отображаемые параметры

Interface	Имя интерфейса, на котором производится логирование.
VLAN	VLAN, на которой производится логирование.
Sender IP	MAC-адрес источника у логируемого ARP.
Occurence	Счетчик общего числа логирования записей, а также времени последнего случившегося логирования.

33. Команды Error Recovery

33-1 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 | bpd-protect | arp-rate | dhcp-rate | loopback-detect | l2pt-guard | duld} [interval SECONDS]
```

```
no errdisable recovery cause {all | psecure-violation | storm-control | bpd-protect | arp-rate | dhcp-rate | loopback-detect | l2pt-guard | duld} [interval SECONDS]
```

Параметры

all	Укажите, чтобы включить опцию Auto-Recovery для всех ситуаций.
psecure-violation	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной Port Security Violation.
storm-control	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной Storm Control.
bpd-protect	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной BPDU Protection.
arp-rate	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной ARP Rate Limiting.
dhcp-rate	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной DHCP Rate Limiting.
loopback-detect	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной Loop Detection.
l2pt-guard	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной L2PT guard.
duld	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной D-Link Unidirectional.
interval SECONDS	Укажите время, необходимое для восстановления порта при ошибке, вызванной указанным модулем. Доступный диапазон значений: от 5 до 86400 секунд. Значение по умолчанию – 300 секунд.

По умолчанию

По умолчанию опция Auto-Recovery отключена для всех ситуаций.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Ошибка на порту может быть вызвана Port Security Violations, Storm Control и так далее. При возникновении ошибки порт отключается, однако для настроек конфигурации будет действовать опция **no shutdown**.

Восстановить порт при возникновении ошибки можно двумя способами. При помощи команды **errdisable recovery cause** администратор может включить функцию Auto-Recovery на портах, отключенных при возникновении конкретных ошибок. Также порт можно восстановить вручную, для этого сначала введите команду **shutdown**, а затем **no shutdown**.

Пример

В данном примере показано, как установить Recovery Timer (таймер восстановления) на 200 секунд для восстановления порта при ошибке, вызванной Port Security Violation.

```
Switch# configure terminal
Switch(config)# errdisable recovery cause psecure-violation interval 200
Switch(config)#
```

В данном примере показано, как включить опцию auto-recovery для восстановления порта при ошибке, вызванной Port Security Violation.

```
Switch# configure terminal
Switch(config)# errdisable recovery cause psecure-violation
Switch(config)#
```

33-2 show errdisable recovery

Данная команда используется для отображения настроек Recovery Timer (таймер восстановления).

```
show errdisable recovery
```

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить настройки Recovery Timer.

Пример

В данном примере показано, как отобразить настройки Recovery Timer.

```
Switch#show errdisable recovery

ErrDisable Cause           State           Interval
-----
Port Security              disabled        300 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
l2pt-guard                 disabled        300 seconds
D-LINK Unidirectional Link Detection disabled        300 seconds

Interfaces that will be recovered at the next timeout:

Interface  Errdisable Cause           Time left(sec)
-----
eth1/0/7   BPDU Attack Protection     infinite
eth2/0/3   Loop Detection              45
eth2/0/5   Loop Detection              45

Switch#
```

33- 3snmp-server enable traps transceiver-monitoring

Данная команда используется для того, чтобы включить отправку SNMP-уведомлений об ошибке на порту. Используйте форму **no**, чтобы отключить отправку уведомлений.

snmp-server enable traps errdisable [asserted] [cleared] [notification-rate TRAP-RATE]
no snmp-server enable traps errdisable [asserted] [cleared] [notification-rate]

Параметры

asserted	(Опционально) Укажите, чтобы включить/отключить отправку SNMP-уведомлений об ошибке на порту.
cleared	(Опционально) Укажите, чтобы включить/отключить отправку SNMP-уведомлений об устранении ошибки.
notification-rate	(Опционально) Укажите количество трапов в минуту. Доступный диапазон значений: от 0 до 1000. Если количество пакетов превысило указанное значение, все последующие пакеты будут отброшены. Если указан 0, ограничения по количеству отсылаемых SNMP-уведомлений об ошибке в минуту отсутствуют.

По умолчанию

По умолчанию данная опция отключена.
Количество уведомлений в минуту по умолчанию – 0.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

При использовании команды без дополнительных параметров будет включена/выключена отправка SNMP-уведомлений об ошибке на порту / устранении ошибки. Если указан только параметр **notification-rate**, будет изменено количество трапов в минуту, при этом настройки отправки уведомлений об ошибке на порту останутся прежними.

Пример

В данном примере показано, как включить отставку SNMP-уведомлений об ошибке на порту.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps errdisable
Switch(config)#
```

34. Команды Ethernet OAM

34-1 ethernet oam

Данная команда используется для включения функции Ethernet OAM на указанном порту. Используйте форму **no**, чтобы отключить данную функцию.

```
ethernet oam
no ethernet oam
```

Параметры

Нет

По умолчанию

По умолчанию функция Ethernet OAM отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

После запуска данной функции на интерфейсе начнется процесс обнаружения OAM. Если на интерфейсе включен активный режим OAM, будет запущено обнаружение. В противном случае порт реагирует на обнаружение, полученное от удаленного узла.

Пример

В данном примере показано, как включить Ethernet OAM на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam
Switch(config-if)#
```

34-2 ethernet oam mode

Данная команда используется для настройки режима Ethernet OAM на указанном порту. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ethernet oam mode {active | passive}
no ethernet oam mode
```

Параметры

active	Укажите, чтобы включить активный режим Ethernet OAM на порту.
passive	Укажите, чтобы включить пассивный режим Ethernet OAM на порту.

По умолчанию

По умолчанию включен активный режим Ethernet OAM.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Следующие два действия разрешены для портов в активном режиме, но запрещены для портов в пассивном режиме:

- Запуск обнаружения OAM
- Запуск/остановка опции Remote Loopback

Пример

В данном примере показано, как включить активный режим Ethernet OAM на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam mode active
Switch(config-if)#
```

34-3 ethernet oam link-monitor error-symbol

Данная команда используется для включения уведомлений о событиях Ethernet OAM Error Symbol, а также для настройки пороговых значений и периода контроля на указанном порту. Используйте форму **no**, чтобы отключить уведомления и вернуться к настройкам по умолчанию.

**ethernet oam link-monitor error-symbol [threshold NUMBER | window DECISECONDS]
no ethernet oam link-monitor error-symbol [threshold | window]**

Параметры

threshold NUMBER	(Опционально) Укажите пороговое количество ошибок кодировки символов в диапазоне от 0 до 4294967295. Если количество ошибок за период времени превысило указанное пороговое значение, будет создано событие Ethernet OAM ErrorSymbol.
window DECISECONDS	(Опционально) Укажите период контроля, в течение которого будет отслеживаться пороговое количество ошибок кодировки символов. Если в течение указанного

периода пороговое значение было превышено, будет создано уведомление OAM PDU с TLV события Error Symbol.
Допустимый диапазон значений: от 10 до 600 децисекунд.

По умолчанию

По умолчанию уведомления о событиях Ethernet OAM Error Symbol включены.

По умолчанию пороговое значение для контроля событий Ethernet OAM Error Symbol – 1.

По умолчанию период контроля событий Ethernet OAM Error Symbol – 10 децисекунд.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Функция Link Monitoring подсчитывает количество ошибок кодировки символов в течение указанного периода. Если количество ошибок равно пороговому значению или превышает его, будет создано событие Ethernet OAM Error Symbol.

Пример

В данном примере показано, как включить уведомления о событиях Ethernet OAM Error Symbol на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-symbol
Switch(config-if)#
```

В данном примере показано, как отключить уведомления о событиях Ethernet OAM Error Symbol на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# no ethernet oam link-monitor error-symbol
Switch(config-if)#
```

В данном примере показано, как настроить пороговое значение для контроля событий Ethernet OAM Error Symbol на порту Ethernet 1/0/1. Указанное значение – 100.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-symbol threshold 100
Switch(config-if)#
```

В данном примере показано, как настроить период контроля событий Ethernet OAM Error Symbol на порту Ethernet 1/0/1. Указанное значение – 100 децисекунд.


```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-symbol window 100
Switch(config-if)#
```

В данном примере показано, как настроить пороговое значение для контроля событий Ethernet OAM Error Symbol на порту Ethernet 1/0/1. Указанное значение – значение по умолчанию.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# no ethernet oam link-monitor error-symbol threshold
Switch(config-if)#
```

34-4 ethernet oam link-monitor error-frame

Данная команда используется для включения уведомлений о событиях Ethernet OAM Error Frame, а также для настройки пороговых значений и периода контроля на указанном порту. Используйте форму **no**, чтобы отключить уведомления и вернуться к настройкам по умолчанию.

**ethernet oam link-monitor error-frame [threshold NUMBER | window DECISECONDS]
no ethernet oam link-monitor error-frame [threshold | window]**

Параметры

threshold NUMBER	(Опционально) Укажите пороговое количество кадров с ошибками в диапазоне от 0 до 4294967295. Если количество кадров с ошибками за период времени превысило указанное пороговое значение, будет создано событие Ethernet OAM Error Frame.
window DECISECONDS	(Опционально) Укажите период контроля, в течение которого будет отслеживаться пороговое количество кадров с ошибками. Если в течение указанного периода пороговое значение было превышено, будет создано уведомление OAM PDU с TLV события Error Frame. Допустимый диапазон значений: от 10 до 600 децисекунд.

По умолчанию

По умолчанию уведомления о событиях Ethernet OAM Error Frame включены.
По умолчанию пороговое значение для контроля событий Ethernet OAM Error Frame – 1.
По умолчанию период контроля событий Ethernet OAM Error Frame – 10 децисекунд.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Функция Link Monitoring подсчитывает количество кадров с ошибками в течение указанного периода контроля. Если количество кадров с ошибками равно пороговому значению или превышает его, будет создано событие Ethernet OAM Error Frame.

Пример

В данном примере показано, как включить уведомления о событиях Ethernet OAM Error Frame на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame
Switch(config-if)#
```

В данном примере показано, как отключить уведомления о событиях Ethernet OAM Error Frame на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# no ethernet oam link-monitor error-frame
Switch(config-if)#
```

В данном примере показано, как настроить пороговое значение для контроля событий Ethernet OAM Error Frame на порту Ethernet 1/0/1. Указанное значение – 100.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame threshold 100
Switch(config-if)#
```

В данном примере показано, как настроить период контроля событий Ethernet OAM Error Frame на порту Ethernet 1/0/1. Указанное значение – 100 децисекунд.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame window 100
Switch(config-if)#
```

В данном примере показано, как настроить период контроля событий Ethernet OAM Error Frame на порту Ethernet 1/0/1. Указанное значение – значение по умолчанию.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# no ethernet oam link-monitor error-frame window
Switch(config-if)#
```

34-5 ethernet oam link-monitor error-frame-seconds

Данная команда используется для включения уведомлений о событиях Ethernet OAM Error FrameSeconds, а также для настройки пороговых значений и периода контроля на указанном порту. Используйте форму **no**, чтобы отключить уведомления и вернуться к настройкам по умолчанию.

**ethernet oam link-monitor error-frame-seconds [threshold NUMBER | window DECISECONDS]
no ethernet oam link-monitor error-frame-seconds [threshold | window]**

Параметры

threshold <i>NUMBER</i>	(Опционально) Укажите пороговое количество кадров с ошибками в диапазоне от 1 до 900 секунд. Если количество кадров с ошибками за период времени превысило указанное пороговое значение, будет создано событие Ethernet OAM Error Frame Seconds.
window <i>DECISECONDS</i>	(Опционально) Укажите период контроля, в течение которого будет отслеживаться пороговое количество кадров с ошибками. Если в течение указанного периода пороговое значение было превышено, будет создано уведомление OAM PDUc TLV события Frame Seconds. Допустимый диапазон значений: от 100 до 9000 децисекунд.

По умолчанию

По умолчанию уведомления о событиях Ethernet OAM Error Frame Seconds включены.
 По умолчанию пороговое значение для контроля событий Ethernet OAM Error Frame Seconds – 1.
 По умолчанию период контроля событий Ethernet OAM Error Frame Seconds – 600 децисекунд.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Функция Link Monitoring подсчитывает количество кадров с ошибками в течение указанного периода.

Если количество кадров с ошибками равно пороговому значению или превышает его, будет создано событие Ethernet OAM Error Frame Seconds. Error Frame Seconds – это интервал в одну секунду, в течение которого был обнаружен по меньшей мере один кадр с ошибкой.

Пример

В данном примере показано, как включить уведомления о событиях Ethernet OAM Error Frame Seconds на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame-seconds
Switch(config-if)#
```

В данном примере показано, как отключить уведомления о событиях Ethernet OAM Error Frame Seconds на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# no ethernet oam link-monitor error-frame-seconds
Switch(config-if)#
```

В данном примере показано, как настроить пороговое значение для контроля событий Ethernet OAM Error Frame Seconds на порту Ethernet 1/0/1. Указанное значение – 100.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame-seconds threshold 100
Switch(config-if)#
```

В данном примере показано, как настроить период контроля событий Ethernet OAM Error Frame Seconds на порту Ethernet 1/0/1. Указанное значение – 100 децисекунд.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame-seconds window 100
Switch(config-if)#
```

В данном примере показано, как настроить пороговое значение для контроля событий Ethernet OAM Error Frame Seconds на порту Ethernet 1/0/1. Указанное значение – значение по умолчанию.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# no ethernet oam link-monitor error-frame-seconds threshold
Switch(config-if)#
```

34-6 ethernet oam link-monitor error-frame-period

Данная команда используется для включения уведомлений о событиях Ethernet OAM Error FramePeriod, а также для настройки пороговых значений и периода контроля на указанном порту. Используйте форму **no**, чтобы отключить уведомления и вернуться к настройкам по умолчанию.

ethernet oam link-monitor error-frame-period [threshold NUMBER | window NUMBER]
no ethernet oam link-monitor error-frame-period [threshold | window]

Параметры

threshold NUMBER	(Опционально) Укажите пороговое количество кадров с ошибками в диапазоне от 0 до 4294967295. Если количество ошибок за период времени превысило указанное пороговое значение, будет создано событие Ethernet OAM Error Frame Period.
window DECISECONDS	(Опционально) Укажите количество кадров для отслеживания порогового значения. Если в течение указанного периода пороговое значение было превышено, будет создано уведомление о событии OAM PDU с TLV события Error Frame Period. Нижняя граница – количество кадров минимального размера, которое можно получить в течение 100 миллисекунд на нижнем физическом слое. Верхняя граница – количество кадров минимального размера, которое можно получить в течение 1 минуты на

нижнем физическом слое.

По умолчанию

По умолчанию уведомления о событиях Ethernet OAM Error Frame Period включены.

По умолчанию пороговое значение для контроля событий Ethernet OAM Error Frame Period – 1.

По умолчанию период для контроля событий Ethernet OAM Error Frame Period – количество кадров минимального размера, которое можно получить в течение 1 секунды на нижнем физическом слое.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Функция Link Monitoring подсчитывает количество кадров с ошибками в течение указанного периода. Период исчисляется количеством полученных кадров. Если количество ошибок равно пороговому значению или превышает его, будет создано событие Ethernet OAM Error Frame Period.

Пример

В данном примере показано, как включить уведомления о событиях Ethernet OAM Error Frame Period на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame-period
Switch(config-if)#
```

В данном примере показано, как отключить уведомления о событиях Ethernet OAM Error Frame Period на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# no ethernet oam link-monitor error-frame-period
Switch(config-if)#
```

В данном примере показано, как настроить пороговое значение для контроля событий Ethernet OAM Error Frame Period на порту Ethernet 1/0/1. Указанное значение – 100.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame-period threshold 100
Switch(config-if)#
```

В данном примере показано, как настроить период контроля событий Ethernet OAM Error Frame Period на порту Ethernet 1/0/1. Указанное значение – 1488100 кадров.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame-period window 1488100
Switch(config-if)#
```

В данном примере показано, как настроить пороговое значение для контроля событий Ethernet OAM Error Frame Period на порту Ethernet 1/0/1. Указанное значение – значение по умолчанию.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# no ethernet oam link-monitor error-frame-period threshold
Switch(config-if)#
```

34-7 ethernet oam remote-failure dying-gasp

Данная команда используется для включения уведомлений о событиях Ethernet OAM Dying Gasp на указанном порту. Используйте форму **no**, чтобы отключить данную функцию.

```
ethernet oam remote-failure dying-gasp
no ethernet oam remote-failure dying-gasp
```

Параметры

Нет

По умолчанию

По умолчанию уведомления о событиях Ethernet OAM Dying Gasp включены.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки событий Dying Gasp. Если данная функция отключена, порт не будет отсылать OAM PDU с набором битов события Dying Gasp при возникновении необратимой локальной неисправности.

Пример

В данном примере показано, как включить уведомления о событиях Dying Gasp на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam remote-failure dying-gasp
Switch(config-if)#
```

34-8 ethernet oam remote-failure critical-event

Данная команда используется для включения уведомлений о событиях Ethernet OAM Critical на указанном порту. Используйте форму **no**, чтобы отключить данную функцию.

```
ethernet oam remote-failure critical-event
no ethernet oam remote-failure critical-event
```

Параметры

Нет

По умолчанию

По умолчанию уведомления о событиях Ethernet OAM Critical включены.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки событий Critical. Если данная функция отключена, порт не будет отсылать OAM PDU с набором битов события Critical при возникновении неустановленного события Critical.

Пример

В данном примере показано, как включить уведомления о событиях Critical на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam remote-failure critical-event
Switch(config-if)#
```

34-9 ethernet oam remote-loopback

Данная команда используется для настройки функции Remote Loopback на указанном порту.

```
ethernet oam remote-loopback {start | stop} interface INTERFACE-ID [, | -]
```

Параметры

start	Укажите, чтобы запросить переход узла в режим Remote Loopback.
stop	Укажите, чтобы запросить переход узла в режим Normal Operation.
interface <i>INTERFACE-ID</i>	Укажите ID интерфейса, на котором необходимо включить функцию Remote Loopback. Доступны только физические порты.
,	(Опционально) Используется для перечисления нескольких

	интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы запросить переход удаленного узла в режим Ethernet OAM Remote Loopback или выход из данного режима. Используйте команду **ethernet oam remote-loopbackstart**, чтобы запросить переход удаленного узла в режим Ethernet OAM Remote Loopback. Используйте команду **ethernet oam remote-loopback stop**, чтобы запросить выход удаленного узла из режима Ethernet OAM Remote Loopback.

Если удаленный узел сконфигурирован так, чтобы игнорировать запросы Remote Loopback, при получении запроса узел не будет входить в режим Remote Loopback или выходить из данного режима. Чтобы запустить переход удаленного узла в режим Remote Loopback, администратору необходимо убедиться, что локальный клиент функционирует в активном режиме и установлено соединение OAM. Если локальный клиент уже перешел в режим Remote Loopback, данная команда неприменима.

Пример

В данном примере показано, как запустить Ethernet OAM Remote Loopback на порту Ethernet 1/0/1.

```
Switch# ethernet oam remote-loopback start interface ethernet 1/0/1
Switch#
```

34- 10 ethernet oam received-remote-loopback

Данная команда используется для настройки режима работы требований Remote Loopback, полученных от узла на указанном порту. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ethernet oam received-remote-loopback {process | ignore}

Параметры

process	Укажите, чтобы реагировать на требования Remote Loopback, полученные от узла.
ignore	Укажите, чтобы игнорировать требования Remote Loopback, полученные от узла.

По умолчанию

По умолчанию Ethernet OAM игнорирует требования Remote Loopback.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную функцию, чтобы выбрать, будет ли клиент обрабатывать полученную команду Ethernet OAM Remote Loopback или игнорировать ее. В режиме Remote Loopback Mode весь пользовательский трафик обрабатываться не будет. Если полученная команда Remote Loopback игнорирована, на порту не будет включен режим Remote Loopback.

Пример

В данном примере показано, как включить обработку команды Ethernet OAM Remote Loopback на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam received-remote-loopback process
Switch(config-if)#
```

34-11 show ethernet oam configuration

Данная команда используется для отображения настроек функции Ethernet OAM.

show ethernet oam configuration [interface *INTERFACE-ID* [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите interface ID физического порта, который необходимо отобразить.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения настроек Ethernet OAM на порту.

Пример

В данном примере показано, как отобразить настройки Ethernet OAM на порту Ethernet 1/0/1.

```
Switch#show ethernet oam configuration interface ethernet 1/0/1

eth1/0/1
  Ethernet oam state      : Disabled
  Mode                   : Active
  Dying gasp             : Enabled
  Critical event         : Enabled
  Remote loopback OAMPDU : Not Processed

  Error symbol period event
    Notify state         : Enabled
    Threshold            : 1 error symbol
    Window               : 10 deciseconds

  Error frame event
    Notify state         : Enabled
    Threshold            : 1 error frame
    Window               : 10 deciseconds

  Error frame period event
    Notify state         : Enabled
    Threshold            : 1 error frame
    Window               : 1488100 frames

  Error frame seconds event

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

34-12 show ethernet oam status

Данная команда используется для отображения статуса функции Ethernet OAM.

show ethernet oam status [interface *INTERFACE-ID* [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите interface ID физического порта, который необходимо отобразить.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона

интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения информации о первичных параметрах и статусе Ethernet OAM на указанных портах.

Пример

В данном примере показано, как отобразить статус Ethernet OAM на порту Ethernet 1/0/1.

```
Switch# show ethernet oam status interface ethernet 1/0/1

eth1/0/1
  Local client
    Admin State           : Enabled
    Mode                  : Active
    Max OAMPDU size       : 1518 bytes
    Remote loopback       : Support
    Unidirectional        : Not support
    Link monitoring       : Support
    Variable request      : Not support
    PDU revision          : 1
    Operation status      : Operational
    Loopback status       : No loopback
  Remote client
    Mode                  : Passive
    MAC address           : 0001.0203.0405
    Vendor (OUI)          : 0180c2
    Max OAMPDU size       : 1518 bytes
    Unidirectional        : Support
    Link monitoring       : Support
    Variable request      : Support
    PDU revision          : 1

Switch#
```

Отображаемые параметры

Max OAMPDU size	Максимальный OAMPDU, поддерживаемый устройством.
------------------------	--

	ОАМ-устройства обмениваются OAMPDU максимального размера и согласовывают использование меньшего из двух максимальных размеров OAMPDU.
PDU revision	Проверка ОАМ-конфигурации, отраженной в последнем отправленном OAMPDU. Используется ОАМ-устройствами для того, чтобы сообщить о произошедших изменениях в конфигурации, которые могут привести к переоценке
Unidirectional	Указывает, что ОАМ-устройство поддерживает передачу OAMPDU по линиям связи, действующим в однонаправленном режиме (трафик проходит только в одном направлении).
Remote loopback	Указывает, что ОАМ-устройство может инициировать команды Loopback и отвечать на них.
Link Monitoring	Указывает, что ОАМ-устройство может отправлять и получать Event Notification OAMPDU.
Variable request	Указывает, что ОАМ-устройство может отправлять и получать различные запросы для контроля атрибутов, описанных в IEEE 802.3 Clause 30 MIB.
Operation status	<p>Disable: ОАМ отключен на данном порту.</p> <p>LinkFault: канал связи обнаружил ошибку и передает уведомления пакеты OAMPDU.</p> <p>PassiveWait: порт находится в пассивном режиме и ожидает устройство с поддержкой ОАМ.</p> <p>ActiveSendLocal: порт находится в активном режиме и отправляет локальную информацию.</p> <p>SendLocalAndRemote: локальный порт обнаружил узел, но еще не принял и не отклонил его настроек.</p> <p>SendLocalAndRemoteOk: локальное устройство принимает ОАМ-обнаружения.</p> <p>PeeringLocallyRejected: локальное ОАМ-устройство отклоняет ОАМ-обнаружения удаленного устройства.</p> <p>PeeringRemotelyRejected: удаленное ОАМ-устройство отклоняет ОАМ-обнаружения локального устройства.</p> <p>Operational: локальное ОАМ-устройство узнает, что локальное и удаленное ОАМ-устройства установили связь.</p> <p>NonOperHalfDuplex: функции Ethernet OAM не работают полностью через полудуплексный порт. Данное значение показывает, что Ethernet OAM включен, но порт работает в полудуплексном режиме.</p>

34-13 show ethernet oam statistics

Данная команда используется для отображения статистики Ethernet OAM.

```
show ethernet oam statistics [interface INTERFACE-ID [, | -]]
```

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите interface ID физического порта, который необходимо отобразить.
--------------------------------------	--

,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения статистики Ethernet OAM на порту.

Пример

В данном примере показано, как отобразить статистику Ethernet OAM на порту Ethernet 1/0/1.

```
Switch#show ethernet oam statistics interface ethernet 1/0/1

eth1/0/1
-----
Information OAMPDU TX           : 0
Information OAMPDU RX           : 0
Unique Event Notification OAMPDU TX : 0
Unique Event Notification OAMPDU RX : 0
Duplicate Event Notification OAMPDU TX: 0
Duplicate Event Notification OAMPDU RX: 0
Loopback Control OAMPDU TX      : 0
Loopback Control OAMPDU RX      : 0
Variable Request OAMPDU TX      : 0
Variable Request OAMPDU RX      : 0
Variable Response OAMPDU TX     : 0
Variable Response OAMPDU RX     : 0
Organization Specific OAMPDU TX : 0
Organization Specific OAMPDU RX : 0
Unsupported OAMPDU TX           : 0
Unsupported OAMPDU RX           : 0
Frames Lost Due To OAM          : 0

Switch#
```

34-14 clear ethernet oam statistics

Данная команда используется для удаления статистики Ethernet OAM.

clear ethernet oam statistics [interface *INTERFACE-ID* [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите interface ID физического порта, который необходимо удалить.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для удаления статистики Ethernet OAM на порту.

Пример

В данном примере показано, как удалить статистику Ethernet OAM на порту Ethernet 1/0/1.

```
Switch# clear ethernet oam statistics interface ethernet 1/0/1
Switch#
```

34-15 show ethernet oam event-log

Данная команда используется для отображения журнала событий Ethernet OAM.

show ethernet oam event-log [interface *INTERFACE-ID* [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите interface ID физического порта, который необходимо удалить.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов.

интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения журнала событий Ethernet OAM на порту.

Пример

В данном примере показано, как отобразить журнал событий Ethernet OAM на порту Ethernet 1/0/1.

```

Switch# show ethernet oam event-log interface ethernet 1/0/1

eth1/0/1
  Local Faults:
  -----
    0 Link Fault records
    0 Dying Gasp records
    0 Critical Event records

  Remote Faults:
  -----
    0 Link Fault records
    2 Dying Gasp records
      Event index          : 2
      Time stamp           : 2013.04.18 10:30
      Event index          : 1
      Time stamp           : 2013.04.18 10:20
    0 Critical Event records

  Local event logs:
  -----
    0 Errored Symbol records
    0 Errored Frame records
    0 Errored Frame Period records
    0 Errored Frame Second records

  Remote event logs:
  -----
    0 Errored Symbol records
    1 Errored Frame records
      Event index          : 3
      Time stamp           : 2013.04.18 10:31
      Error frame          : 5
      Window               : 10 (decisecond)
      Threshold            : 3
      Accumulated errors   : 10
    0 Errored Frame Period records
    0 Errored Frame Second records

Switch#

```

Отображаемые параметры

Event index	Индекс события.
Time stamp	Время создания события.
Error frame	Количество кадров с ошибками, обнаруженных за указанный период.
Window	Продолжительность периода в интервалах 100 миллисекунд.
Threshold	Пороговое значение. Если количество кадров с ошибками, обнаруженных за указанный период, равно пороговому значению или превышает его, будет создано событие.
Accumulated errors	Сумма записей об ошибках, обнаруженных в данном

событии с момента сброса подуровня OAM.

35-16 clear ethernet oam event-log

Данная команда используется для очистки журнала событий Ethernet OAM.

clear ethernet oam event-log [interface *INTERFACE-ID* [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите interface ID физического порта, который необходимо удалить.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для очистки журнала событий Ethernet OAM на порту.

Пример

В данном примере показано, как очистить журнал событий Ethernet OAM на порту Ethernet 1/0/1.

```
Switch# clear ethernet oam event-log interface ethernet 1/0/1
Switch#
```

35. Команды Ethernet Ring Protection Switching (ERPS)

35-1 description

Данная команда используется для указания строки, которая служит описанием для кольца G.8032 Ethernet.

description *DESCRIPTION*

Параметры

<i>DESCRIPTION</i>	Укажите описание для кольца G.8032 Ethernet. Максимально допустимое количество символов – 64.
--------------------	--

По умолчанию

Нет

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить строку описания для экземпляра ERPS.

Пример

В данном примере показано, как создать ERPS-экземпляр 1 в физическом кольце «major-ring» и добавить описание для экземпляра.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#description major-ring instance 1
Switch(config-erps-ring-instance)#
```

35-2 ethernet ring g8032

Данная команда используется для создания физического кольца G.8032 и перехода в режим ERPS Configuration Mode. Используйте форму **no**, чтобы удалить физическое кольцо G.8032.

ethernet ring g8032 *RING-NAME*
no ethernet ring g8032 *RING-NAME*

Параметры

<i>RING-NAME</i>	Укажите имя кольца G.8032. Максимально допустимое количество символов – 32.
------------------	---

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы создать или изменить кольцо G.8032 и войти в режим ERPS Configuration Mode. Кольцо, созданное при помощи команды, представляет собой физическое кольцо.

Пример

В данном примере показано, как создать кольцо G.8032 «major-ring».

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#
```

35-3 ethernet ring g8032 profile

Данная команда используется для создания профиля G.8032 и входа в режим G.8032 Profile Configuration Mode. Используйте форму **no**, чтобы удалить профиль G.8032.

```
ethernet ring g8032 profile PROFILE-NAME
no ethernet ring g8032 profile PROFILE-NAME
```

Параметры

<i>PROFILE-NAME</i>	Укажите имя профиля G.8032. Максимально допустимое количество символов – 32.
---------------------	--

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы создать или изменить профиль G.8032 и войти в режим G.8032 Profile Configuration Mode.

Пример

В данном примере показано, как создать профиль G.8032 «campus».

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 profile campus
Switch(config-erps-ring-profile)#timer guard 700
Switch(config-erps-ring-profile)#timer hold-off 1
Switch(config-erps-ring-profile)#timer wtr 1
Switch(config-erps-ring-profile)#
```

35-4 tcn-propagation

Данная команда используется для включения передачи уведомлений об изменении топологии (TCN) от экземпляра sub-ERPS к основному экземпляру. Используйте форму **no**, чтобы отключить передачу уведомлений об изменении топологии.

tcn-propagation
no tcn-propagation

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

G.8032 Profile Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить передачу уведомлений об изменении топологии от экземпляра подкольца к другим экземплярам кольца.

Пример

В данном примере показано, как включить передачу TCN для профиля G.8032 «campus».

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 profile campus
Switch(config-erps-ring-profile)#tcn-propagation
Switch(config-erps-ring-profile)#
```

35-5 r-aps channel-vlan

Данная команда используется для настройки ERPS R-APS VLAN. Используйте форму **no**, чтобы удалить настройки.

```
r-aps channel-vlan VLAN-ID
no r-aps channel-vlan
```

Параметры

<i>VLAN-ID</i>	Укажите ID R-APS VLAN для экземпляра ERPS. Доступный диапазон значений: от 1 до 4094.
----------------	---

По умолчанию

Нет

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы назначить R-APS VLAN для экземпляра ERPS. Создать и назначить R-APS VLAN необходимо до того, как для экземпляра ERPS будет включен рабочий режим.

У каждого экземпляра ERPS должна быть отдельная R-APS VLAN.

R-APS VLAN экземпляра подкольца также является виртуальным каналом подкольца.

Пример

В данном примере показано, как настроить R-APS VLAN ERPS-экземпляра 1 как VLAN 2.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 ring2
Switch(config-erps-ring)# exit
Switch(config)# ethernet ring g8032 ring1
Switch(config-erps-ring)# sub-ring ring2
Switch(config-erps-ring)# exit
Switch(config)# ethernet ring g8032 ring2
Switch(config-erps-ring)# port0 interface eth3/0/1
Switch(config-erps-ring)# port1 none
Switch(config-erps-ring)# instance 1
Switch(config-erps-ring-instance)# x-aps channel-vlan 2
Switch(config-erps-ring-instance)#
```

35-6 inclusion-list vlan-ids

Данная команда используется для определения заданных VLAN ID, которые защищены механизмом Ethernet Ring Protection. Используйте форму **no**, чтобы удалить заданные VLAN ID.

inclusion-list vlan-ids *VLAN-ID* [, | -]
no inclusion-list vlan-ids *VLAN-ID* [, | -]

Параметры

<i>VLAN-ID</i>	Укажите VLAN ID защищенных VLAN экземпляра ERPS. Доступный диапазон значений: от 1 до 4094.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы сконфигурировать защиту VLAN при помощи экземпляра ERPS.

Пример

В данном примере показано, как сконфигурировать защищенные сервисом Ethernet Ring Protection VLAN 100-200 для ERPS-экземпляра 1.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 ring2
Switch(config-erps-ring)# port0 interface ethernet 1/0/1
Switch(config-erps-ring)# port1 none
Switch(config-erps-ring)# instance 1
Switch(config-erps-ring-instance)# r-aps channel-vlan 20
Switch(config-erps-ring-instance)# inclusion-list vlan-ids 100-200
Switch(config-erps-ring-instance)#
```

35-7 instance

Данная команда используется для создания экземпляра ERPS и входа в режим ERPS Instance Configuration Mode. Используйте форму **no**, чтобы удалить экземпляр ERPS.

instance *INSTANCE-ID*
no instance *INSTANCE-ID*

Параметры

<i>INSTANCE-ID</i>	Укажите идентификатор экземпляра ERPS в диапазоне от 1 до 32.
--------------------	---

По умолчанию

Нет

Режим ввода команды

ERPS Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для того, чтобы создать экземпляр ERPS в физическом кольце. Используйте несколько экземпляров в одном физическом кольце, чтобы распределить нагрузку. ID экземпляров ERPS в физических кольцах системы являются глобально значимыми.

Пример

В данном примере показано, как создать ERPS-экземпляр 1 в физическом кольце «major-ring».

```
Switch(config)# ethernet ring g8032 major-ring
Switch(config-erps-ring)# port0 interface ethernet 1/0/1
Switch(config-erps-ring)# port1 none
Switch(config-erps-ring)# instance 1
Switch(config-erps-ring-instance)#
```

35-8 level

Данная команда используется для настройки значения MEL кольца экземпляра ERPS. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

level MEL-VALUE
no level

Параметры

<i>MEL-VALUE</i>	Укажите значение MEL кольца экземпляра ERPS в диапазоне от 0 до 7.
------------------	--

По умолчанию

Значение по умолчанию – 1.

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Значение MEL кольца всех узлов в одном экземпляре ERPS должно быть идентичным.

Пример

В данном примере показано, как настроить значение MEL кольца ERPS-экземпляра 1. Указанное значение – 6.

```
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#port0 interface ethernet 1/0/1
Switch(config-erps-ring)#port1 none
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#level 6
Switch(config-erps-ring-instance)#
```

35-9 sub-ring

Данная команда используется для указания экземпляра подкольца по умолчанию экземпляра для физического экземпляра кольца по умолчанию. Используйте форму **no**, чтобы удалить экземплярподкольца по умолчанию.

sub-ring SUB-RING-NAME
no sub-ring SUB-RING-NAME

Параметры

<i>SUB-RING-NAME</i>	Укажите имя подкольца G8032.
----------------------	------------------------------

По умолчанию

Нет

Режим ввода команды

ERPS Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Настройте подкольцо, подключенное к другому кольцу. Данная команда применяется на связный узел.

Пример

В данном примере показано, как настроить физическое кольцо «ring2» в качестве подкольца «ring1».

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 ring2
Switch(config-erps-ring)# exit
Switch(config)# ethernet ring g8032 ring1
Switch(config-erps-ring)# sub-ring ring2
Switch(config-erps-ring)#
```

35-10 sub-ring instance

Данная команда используется для указания экземпляра подкольца для экземпляра физического кольца. Используйте форму **no**, чтобы удалить экземпляр подкольца для экземпляра физического кольца.

```
sub-ring instance INSTANCE-ID
no sub-ring instance INSTANCE-ID
```

Параметры

<i>INSTANCE-ID</i>	Укажите идентификатор экземпляра ERPS в диапазоне от 1 до 32.
--------------------	---

По умолчанию

Нет

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить экземпляр подкольца, подключенный к другому экземпляру кольца. Данная команда применяется на связанный узел.

Пример

В данном примере показано, как настроить экземпляр 1 физического кольца «ring2» в качестве подкольца экземпляра 2 «ring1».

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 ring2
Switch(config-erps-ring)# instance 1
Switch(config-erps-ring-instance)# exit
Switch(config-erps-ring)# exit
Switch(config)# ethernet ring g8032 ring1
Switch(config-erps-ring)#instance 2
Switch(config-erps-ring-instance)# sub-ring instance 1
Switch(config-erps-ring-instance)#
```

35-11 profile

Данная команда используется для привязки экземпляра ERPS к профилю G.8032. Используйте форму **no**, чтобы удалить привязку.

profile *PROFILE-NAME*
no profile

Параметры

<i>PROFILE-NAME</i>	Укажите имя профиля G.8032, к которому необходимо привязать экземпляр ERPS.
---------------------	---

По умолчанию

Нет

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Перед изменением привязки профиля необходимо отключить экземпляр ERPS.

Пример

В данном примере показано, как настроить значения таймеров для профиля «campus», а затем привязать экземпляр 1 и экземпляр 2 к профилю. Для Guard Timer указано значение 700 миллисекунд, для Hold-Off Timer – 1 секунда, для WTR Timer – 1 минута.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 profile campus
Switch(config-erps-ring-profile)# timer guard 700
Switch(config-erps-ring-profile)# timer hold-off 1
Switch(config-erps-ring-profile)# timer wtr 1
Switch(config-erps-ring-profile)# exit
Switch(config)# ethernet ring g8032 ring1
Switch(config-erps-ring)# port0 interface eth3/0/1
Switch(config-erps-ring)# port1 interface eth3/0/2
Switch(config-erps-ring)# instance 1
Switch(config-erps-ring-instance)# profile campus
Switch(config-erps-ring-instance)# exit
Switch(config-erps-ring)# exit
Switch(config)# ethernet ring g8032 ring2
Switch(config-erps-ring)# exit
Switch(config)# ethernet ring g8032 ring1
Switch(config-erps-ring)# sub-ring ring2
Switch(config-erps-ring)# exit
Switch(config)# ethernet ring g8032 ring2
Switch(config-erps-ring)# port0 interface eth3/0/3
Switch(config-erps-ring)# port1 none
Switch(config-erps-ring)# instance 2
Switch(config-erps-ring-instance)# profile campus
Switch(config-erps-ring-instance)#
```

35-12 port0

Данная команда используется для указания первого порта физического кольца. Используйте форму **no**, чтобы удалить заданные настройки.

```
port0 interface INTERFACE-ID
no port0
```

Параметры

<i>INTERFACE-ID</i>	Укажите interface ID порта кольца. Доступны физические порты и port-channel.
---------------------	--

По умолчанию

Нет

Режим ввода команды

ERPS Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить первый порт физического кольца.

Пример

В данном примере показано, как настроить порт Ethernet 1/0/1 в качестве первого порта кольца G.8032 «major-ring».

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#port0 interface ethernet 1/0/1
Switch(config-erps-ring)#
```

35-13 port1

Данная команда используется для указания второго порта физического кольца. Используйте форму **no**, чтобы удалить заданные настройки.

port1 {interface *INTERFACE-ID* | none}
no port1

Параметры

<i>INTERFACE-ID</i>	Укажите второй порт кольца. Доступны физические порты и port-channel.
none	Укажите, чтобы настроить связанный узел в качестве конечного локального узла подкольца.

По умолчанию

Нет

Режим ввода команды

ERPS Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить второй порт физического кольца. Используйте команду **port1 none**, чтобы настроить связанный узел в качестве конечного локального узла подкольца.

Пример

В данном примере показано, как настроить связанный узел в качестве конечного локального узла кольца G.8032 «ring2».

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 ring2
Switch(config-erps-ring)# exit
Switch(config)# ethernet ring g8032 ring1
Switch(config-erps-ring)# sub-ring ring2
Switch(config-erps-ring)# exit
Switch(config)# ethernet ring g8032 ring2
Switch(config-erps-ring)# port1 none
Switch(config-erps-ring)#
```

35-14 revertive

Данная команда используется для возвращения к действующему средству передачи в случае устранения неисправности. Используйте форму no, чтобы продолжить использование RPL, при условии его исправности, после устранения ошибки на коммутаторе.

revertive
no revertive

Параметры

Нет

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

G.8032 Profile Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

После того как неисправность коммутатора будет устранена, канал трафика восстанавливается по истечении времени WTR Timer, который используется для предотвращения частого переключения порта, если соединение на каком-то участке кольца очень часто меняет состояние. Если реверсивный режим выключен, после устранения ошибки канал трафика продолжает использовать RPL при условии его исправности.

С учетом защиты Ethernet-кольца ресурсы действующих средств передачи могут быть оптимизированы, в некоторых случаях рекомендуется вернуться к действующему средству передачи, как только будут доступны все кольцевые соединения.

Это выполняется за счет дополнительного разрыва соединения. В некоторых случаях нет преимуществ в немедленном возврате к действующим средствам передачи данных. При этом можно избежать второго разрыва, если не восстанавливать защитное переключение.

Пример

В данном примере показано, как включить нереверсивный режим для колец профиля «campus».

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 profile campus
Switch(config-erps-ring-profile)# no revertive
Switch(config-erps-ring-profile)#
```

35-15 rpl

Данная команда используется для настройки узла в качестве RPL Owner или RPL Neighbor, а также для назначения порта RPL. Используйте форму **no**, чтобы удалить настройки RPL.

```
rpl {port0 | port1} [owner | neighbor]
no rpl
```

Параметры

port0	Укажите, чтобы настроить порт 0 в качестве порта RPL.
port1	Укажите, чтобы настроить порт 1 в качестве порта RPL.
owner	(Опционально) Укажите, чтобы настроить узел кольца в качестве RPL Owner для сконфигурированного экземпляра.
neighbor	(Опционально) Укажите, чтобы настроить узел кольца в качестве RPL Neighbor для сконфигурированного экземпляра.

По умолчанию

Нет

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать узел кольца в качестве RPL Owner или RPL Neighbor, а кольцевой порт – в качестве порта RPL.

Пример

В данном примере показано, как включить RPL Owner и настроить порт 0 в качестве порта RPL ERPS-экземпляра 1.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 major-ring
Switch(config-erps-ring)# port0 interface eth3/0/1
Switch(config-erps-ring)# port1 interface eth3/0/2
Switch(config-erps-ring)# instance 1
Switch(config-erps-ring-instance)# rpl port0 owner
Switch(config-erps-ring-instance)#
```

35-16 show ethernet ring g8032

Данная команда используется для отображения информации об экземпляре ERPS.

```
show ethernet ring g8032 status [RING-NAME] [instance [INSTANCE-ID]]
show ethernet ring g8032 brief [RING-NAME] [instance [INSTANCE-ID]]
show ethernet ring g8032 profile [PROFILE-NAME]
```

Параметры

<i>RING-NAME</i>	(Опционально) Укажите, чтобы отобразить информацию о физическом кольце ERPS.
<i>PROFILE-NAME</i>	(Опционально) Укажите, чтобы отобразить информацию о профиле ERPS.
<i>INSTANCE-ID</i>	(Опционально) Укажите, чтобы отобразить информацию об экземпляре ERPS.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию об ERPS.

Пример

В данном примере показано, как отобразить подробную информацию об ERPS.

```
Switch#show ethernet ring g8032 status

ERPS Version: G.8032v2
-----
Ethernet Ring ring1
Admin Port0: eth3/0/1
Admin Port1: eth3/0/2
Ring Type: Major ring
Ring ID: 1
-----
Instance : 1
Instance Status: Idle
R-APS Channel : 2,Protected VLANs:3
Port0: eth3/0/1, Blocking
Port1: eth3/0/2, Forwarding
Profile: 1
Description :
Guard Timer: 500 milliseconds
Hold-off Timer: 0 milliseconds
WTR Timer: 1 minutes
Revertive
MEL: 1
RPL Role: Owner
RPL Port: Port0
Sub Ring Instance: none

Switch#
```

В данном примере показано, как отобразить подробную информацию о физическом кольце ERPS «ring1».


```
Switch#show ethernet ring g8032 status ring1

Ethernet Ring ring1
Admin Port0: eth3/0/1
Admin Port1: eth3/0/2
Ring Type: Major ring
Ring ID: 1
-----
Instance : 1
Instance Status: Idle
R-APS Channel : 2,Protected VLANs:3
Port0: eth3/0/1, Blocking
Port1: eth3/0/2, Forwarding
Profile: 1
Description :
Guard Timer: 500 milliseconds
Hold-off Timer: 0 milliseconds
WTR Timer: 1 minutes
Revertive
MEL: 1
RPL Role: Owner
RPL Port: Port0
Sub Ring Instance: none

Switch#
```

В данном примере показано, как отобразить подробную информацию о профиле ERPS «file1».

```
Switch# show ethernet ring g8032 profile file1

Ethernet Ring Profile file1
Guard Timer: 500 milliseconds
Hold-off Timer: 0 milliseconds
WTR Timer: 5 minutes

Switch#
```

В данном примере показано, как отобразить подробную информацию об экземпляре 1 основного кольца физического кольца ERPS.

```
Switch# show ethernet ring g8032 status major-ring instance 1

Instance : 1
Instance Status: Deactivated
R-APS Channel : 0,Protected VLANs:
Port0: eth1/0/1, Forwarding
Port1: eth1/0/2, Forwarding
Profile: file1
Description :
Guard Timer: 500 milliseconds
Hold-off Timer: 0 milliseconds
WTR Timer: 5 minutes
Revertive
MEL: 1
RPL Role: None
RPL Port: -
Sub Ring Instance: none

Switch#
```

В данном примере показано, как отобразить краткую информацию о физическом кольце ERPS «ring1».

```
Switch#show ethernet ring g8032 brief ring1

ERPS Version : G.8032v2
Ring
----
ring1          InstID  Status      Port-State
                ----   -
                1      Deactivated p0:eth1/0/3,Forwarding
                p1:eth1/0/2,Forwarding

Switch#
```

В данном примере показано, как отобразить краткую информацию об экземпляре 1 физического кольца ERPS «ring1».

```
Switch#show ethernet ring g8032 brief ring1 instance 1

ERPS Version : G.8032v2
Ring
----
ring1          InstID  Status      Port-State
                ----   -
                1      Deactivated p0:eth1/0/3,Forwarding
                p1:eth1/0/2,Forwarding

Switch#
```

Отображаемые параметры

MEL	Значение MEL кольца экземпляра ERPS.
R-APS Channel	R-APS VLAN экземпляра ERPS.
Protected VLANs	Защищенные VLAN экземпляра ERPS.
Profile	Профиль, ассоциированный с экземпляром ERPS.
Guard Timer	Значение Guard Timer профиля.
Hold-Off Timer	Значение Hold-Off Timer профиля.

WTR Timer	Значение WTR Timer профиля.
TC Propagation State	ТС распространяются / не распространяются в кольце.
Revertive / Non-revertive	Реверсивный/нереверсивный режим работы колец.
Instance Status	Текущий статус узла кольца экземпляра ERPS. (Deactivated / Init / Idle / Protection / force / manual / pending).
RPL Role	Текущая роль узла экземпляра ERPS. (Owner / Neighbor / None).
Port0 / Port1	Текущая роль кольцевого порта. (Interface_id / virtual_channel).
RPL Port	Текущие настройки RPL. (Port0 / Port1 / None).
Ring port0/port1 state	Статус кольцевых портов экземпляра ERPS. (Forwarding / Blocking / SF / SF blocked).
RingType	Тип кольца (основное кольцо / подкольцо).

35-17 activate

Данная команда используется для включения экземпляра ERPS. Используйте форму **no**, чтобы отключить экземпляр ERPS.

```
activate
no activate
```

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить экземпляр ERPS. Перед этим необходимо настроить кольцевые порты и APS Channel.

В дополнение к данным настройкам, для работы экземпляра ERPS необходимы настройки защищенных VLAN и RPL.

Пример

В данном примере показано, как включить экземпляр 1 основного кольца.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 major-ring
Switch(config-erps-ring)# instance 1
Switch(config-erps-ring-instance)# profile campus
Switch(config-erps-ring-instance)# activate
Switch(config-erps-ring-instance)#
```

35-18 timer

Данная команда используется для того, чтобы настроить таймеры для профиля ERPS. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
timer {guard MILLI-SECONDS | hold-off SECONDS | wtr MINUTES}
no timer [guard | hold-off | wtr]
```

Параметры

guard <i>MILLI-SECONDS</i>	Укажите значение Guard Timer в диапазоне от 10 до 2000 миллисекунд. Указанное значение должно быть кратным 10.
hold-off <i>SECONDS</i>	Укажите значение Hold-Off Timer в диапазоне от 0 до 10 секунд.
wtr <i>MINUTES</i>	Укажите значение WTR Timer в диапазоне от 1 до 12 минут.

По умолчанию

Значение Guard Timer по умолчанию – 500 миллисекунд.

Значение Hold-Off Timer по умолчанию – 0.

Значение WTR Timer по умолчанию – 5 минут.

Режим ввода команды

G.8032 Profile Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить значения таймеров, используемых экземплярами ERPS, привязанными к профилю. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию. При использовании формы **no** без указания параметров значения всех таймеров будут сброшены.

Пример

В данном примере показано, как настроить значения таймеров для профиля «campus». Значение Guard Timer – 700 миллисекунд, Hold-Off Timer – 1 секунда, WTR Timer – 1 минута.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 profile campus
Switch(config-erps-ring-profile)#timer guard 700
Switch(config-erps-ring-profile)#timer hold-off 1
Switch(config-erps-ring-profile)#timer wtr 1
Switch(config-erps-ring-profile)#
```

35-19 ring_id

Данная команда используется для указания ID физического кольца. Используйте форму **no**, чтобы удалить настройки.

```
ring_id RING_ID
no ring_id
```

Параметры

<i>RING_ID</i>	Укажите идентификатор физического кольца в диапазоне от 1 до 239.
----------------	---

По умолчанию

Нет

Режим ввода команды

ERPS Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить ID физического кольца. В ERPSv2 каждому физическому кольцу должен быть назначен другой ID кольца.

Данная команда используется только в версии ERPSv2.

Пример

В данном примере показано, как настроить значение кольца G8032 «ring2». Указанное значение – 2.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#ring_id 2
Switch(config-erps-ring)#
```

35-20 ring_type

Данная команда используется для указания типа физического кольца. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ring_type {major-ring | sub-ring}
no ring_type
```

Параметры

major-ring	Укажите кольцо ERPS в качестве основного кольца.
sub-ring	Укажите кольцо ERPS в качестве подкольца.

По умолчанию

Тип кольца ERPS по умолчанию – основное кольцо.

Режим ввода команды

ERPS Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать тип кольца (открытый/закрытый).
Данная команда используется только в версии ERPSv2.

Пример

В данном примере показано, как настроить связанный узел «ring2» в качестве подкольца.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#ring_type sub-ring
Switch(config-erps-ring)#
```

35-21 erps force switch ring_port

Данная команда используется для блокировки порта экземпляра ERPS.

```
erps force switch ring_port {port0 | port1}
```

Параметры

port0	Укажите, чтобы заблокировать порт 0.
port1	Укажите, чтобы заблокировать порт 1.

По умолчанию

Нет

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы принудительно заблокировать порт экземпляра. После применения команды порт будет незамедлительно заблокирован вне зависимости от того, произошел ли разрыв соединения, или нет. Данная команда используется только в версии ERPSv2.

Пример

В данном примере показано, как принудительно заблокировать основное кольцо, экземпляр 1 и порт 0.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#erps force switch ring_port port0
Switch(config-erps-ring-instance)#
```

35-22 erps manual switch ring_port

Данная команда используется для блокировки порта экземпляра ERPS.

erps manual switch ring_port {port0 | port1}

Параметры

port0	Укажите, чтобы вручную заблокировать порт 0 экземпляра ERPS.
port1	Укажите, чтобы вручную заблокировать порт 1 экземпляра ERPS.

По умолчанию

Нет

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы принудительно заблокировать порт, на котором настроена MS, во время сбоя соединения и при отсутствии настроек FS.

Данная команда используется только в версии ERPSv2.

Пример

В данном примере показано, как вручную заблокировать основное кольцо, экземпляр 1 и порт 0.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#erps manual switch ring_port port0
Switch(config-erps-ring-instance)#
```

35-23 clear

Данная команда используется для удаления активной локальной команды администратора.

clear

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

ERPS Instance Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду **clear**, чтобы удалить последствия применения команд **force** и **manual**. Данная команда выполняет следующие функции:

- Запускает реверсивное переключение до момента истечения WTR timer / WTB timer в реверсивном режиме работы.
- Запускает реверсивное переключение в нереверсивном режиме работы.

Данная команда используется только в версии ERPSv2.

Пример

В данном примере показано, как удалить локальные команды, сконфигурированные вручную, для экземпляра 1 основного кольца.


```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#erps manual switch ring_port port0
Switch(config-erps-ring-instance)#clear
Switch(config-erps-ring-instance)#
```

36. Команды File System

36-1 cd

Данная команда используется для смены текущего каталога.

```
cd [DIRECTORY-URL]
```

Параметры

<i>DIRECTORY-URL</i>	(Опционально) Укажите путь к каталогу. Если путь не указан, будет отображен текущий каталог.
----------------------	--

По умолчанию

По умолчанию текущим каталогом является корневой каталог в файловой системе внутренней памяти.

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Если путь не указан, текущий каталог не будет сменен.

Пример

В данном примере показано, как сменить текущий каталог на каталог «d» в файловой системе.

```
Switch#dir

Directory of /c:
 1  -rw      12785484 Jan 15 2000 01:41:56 runtime.had
 2  -rw         35856 Jan 20 2000 04:58:06 config.cfg
 3  -rw      12799156 Jan 20 2000 04:57:18 firmware.had
 4  -rw      12481700 Jan 15 2000 23:57:11 fw5.had
 5  -rw      12791928 Jan 05 2000 23:09:30 backup.had
 6  d--          0 Jan 23 2000 03:49:07 system

125304832 bytes total (70426624 bytes free)

Switch#cd d:
Switch#
```

В данном примере показано, как отобразить текущий каталог.

```
Switch#cd
Current directory is /c:
Switch#
```

36-2 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Файл программного обеспечения или файл конфигурации, указанный в качестве загрузочного файла, удалить невозможно.

Пример

В данном примере показано, как удалить файл «test.txt» из файловой системы внутренней памяти.

```
Switch# delete c:/test.txt
Delete test.txt? (y/n) [n] y
File is deleted
Switch#
```

36-3 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

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Если путь не указан, будет использован текущий каталог. По умолчанию текущий каталог расположен в корне файловой системы внутренней памяти. Накопитель установлен в файловой системе и отображается пользователю в качестве подкаталога корневого каталога.

Используйте команду **dir** для корневого каталога, чтобы отобразить поддерживаемые файловые системы. Используйте команду **show storage media**, чтобы отобразить накопитель, привязанный к файловой системе.

Пример

В данном примере показано, как отобразить корневой каталог автономного коммутатора.

```
Switch#dir /
Directory of /
1  d--          0 Jan 23 2000 03:49:07  c:
0 bytes total (0 bytes free)
Switch#
```

36-4 format

Данная команда используется для форматирования внешнего устройства хранения информации.

format *FILE-SYSTEM* [**fat32** | **fat16**]

Параметры

<i>FILE-SYSTEM</i>	Укажите файловую систему.
fat32	(Опционально) Укажите, чтобы выбрать форматирование в файловую систему FAT32.
fat16	(Опционально) Укажите, чтобы выбрать форматирование в файловую систему FAT16.

По умолчанию

Формат по умолчанию – FAT32.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Отформатировать можно только внешнее устройство хранения информации. По умолчанию накопитель будет отформатирован в файловую систему FAT32.

Пример

В данном примере показано, как отформатировать внешнюю карту Compact Flash.

```
Switch# format /d:
All sectors will be erased, proceed? (y/n) [n] y
Enter volume id (up to 11 characters):Profiles
Format completed.
Switch#
```

36-5 mkdir

Данная команда используется для создания каталога в текущем каталоге.

mkdir *DIRECTORY-NAME*

Параметры

<i>DIRECTORY-NAME</i>	Укажите имя каталога.
-----------------------	-----------------------

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы создать каталог в текущем каталоге.

Пример

В данном примере показано, как создать каталог «newdir» в текущем каталоге.

```
Switch# mkdir newdir
Switch#
```

36-6 more

Данная команда используется для отображения содержимого файла.

more *FILE-URL*

Параметры

<i>FILE-URL</i>	Укажите путь к файлу, который необходимо отобразить.
-----------------	--

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы отобразить содержимое файла в файловой системе. Обычно команда применяется для отображения текстовых файлов. Нестандартные печатные символы будут отображены как нечитаемые знаки или пробелы.

Пример

В данном примере показано, как отобразить содержимое файла «usr_def.conf».

```

Switch# more /c:/configuration/usr_def.conf

!DGS-3130
!Firmware Version: 1.00.001
!Slot      Model
!-----
! 1        DGS-3130-30TS
! 2        -
! 3        DGS-3130-30TS
! 4        DGS-3130-30TS
!
ip igmp snooping vlan 1
!.
end

Switch#

```

36-7 rename

Данная команда используется для переименования файла.

rename *FILE-URL1* *FILE-URL2*

Параметры

<i>FILE-URL1</i>	Укажите путь к файлу, который необходимо переименовать.
<i>FILE-URL2</i>	Укажите путь к переименованному файлу.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Переименованный файл может располагаться в том же или другом каталоге.

Пример

В данном примере показано, как изменить имя файла с «doc.1» на «test.txt».

```
Switch# rename /c:/doc.1 /c:/test.txt
Rename file doc.1 to test.txt? (y/n) [n] y
Switch#
```

36-8 rmdir

Данная команда используется для удаления каталога из файловой системы.

rmdir *DIRECTORY-NAME*

Параметры

<i>DIRECTORY-NAME</i>	Укажите имя каталога, который необходимо удалить.
-----------------------	---

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы удалить каталог из текущего каталога.

Пример

В данном примере показано, как удалить каталог «newdir» из текущего каталога.

```
Switch# rmdir newdir
Remove directory newdir? (y/n) [n] y
The directory is removed
Switch#
```

36-9 show storage media-info

Данная команда используется для отображения информации о накопителе.

show storage media-info [unit *UNIT-ID*]

Параметры

unit UNIT-ID (Опционально) Укажите Unit ID устройства в стеке. Если Unit ID не указан, будут отображены все устройства.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию о доступных накопителях системы.

Пример

В данном примере показано, как отобразить информацию о доступных накопителях на всех устройствах стека.

```
Switch# show storage media-info

Unit  Drive  Media-Type  Size    FS-Type  Label
----  -
1     c:      FLASH      31M     FFS
2     c:      FLASH      31M     FFS
2     d:      SD Card    256M    FAT32    test
3     c:      FLASH      31M     FFS

Switch#
```

Отображаемые параметры

Media-Type	FLASH: Отображает внутреннюю память коммутатора. SD Card: Отображает съемные носители, включая флэш-накопители USB.
-------------------	--

37. Команды Filter Database (FDB)

37-1 clear mac-address-table

Данная команда используется для удаления указанного динамического MAC-адреса, всех динамических MAC-адресов на указанном интерфейсе, всех динамических MAC-адресов на указанной VLAN или всех динамических MAC-адресов из таблицы MAC-адресов.

```
clear mac-address-table dynamic {all | address MAC-ADDR | interface INTERFACE-ID | vlan VLAN-ID}
```

Параметры

all	Укажите, чтобы удалить все динамические MAC-адреса.
address MAC-ADDR	Укажите, чтобы удалить указанный динамический MAC-адрес.
interface INTERFACE-ID	Укажите интерфейс (физический порт или port-channel), на котором необходимо удалить MAC-адрес.
vlan VLAN-ID	Укажите VLAN ID в диапазоне от 1 до 4094.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы удалить записи динамических MAC-адресов. Будет удален только динамический индивидуальный адрес.

Пример

В данном примере показано, как удалить MAC-адрес 00:08:00:70:00:07 из таблицы динамических MAC-адресов.

```
Switch# clear mac-address-table dynamic address 00:08:00:70:00:07
Switch#
```

37-2 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Укажите время устаревания 0, чтобы отключить функцию устаревания MAC-адресов в таблице.

Пример

В данном примере показано, как установить значение времени устаревания на 200 секунд.

```
Switch# configure terminal
Switch(config)# mac-address-table aging-time 200
Switch(config)#
```

37-3 mac-address-table aging destination-hit

Данная команда используется для включения функции Destination MAC Address Triggered Update. Используйте форму **no**, чтобы отключить данную функцию.

mac-address-table aging destination-hit
no mac-address-table aging destination-hit

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Функция source MAC Address Triggered Update всегда включена. Hit Bit записей MAC-адреса, соответствующего порту, получающему пакет, будет обновлен на основании MAC-адреса источника (source) и VLAN пакета. Если пользователь включает функцию Destination MAC Address Triggered Update при помощи команды **mac-address-table aging destination-hit**, Hit Bit записей MAC-адреса, соответствующего порту, передающему пакет, будет обновлен на основании MAC-адреса назначения (destination) и VLAN пакета.

Функция Destination MAC Address Triggered Update увеличивает частоту обновления Hit Bit записей MAC-адреса и уменьшает лавинное распространение трафика при помощи времени устаревания записей MAC-адреса.

Пример

В данном примере показано, как включить функцию Destination MAC Address Triggered Update.

```
Switch# configure terminal
Switch(config)# mac-address-table aging destination-hit
Switch(config)#
```

37-4 mac-address-table learning

Данная команда используется для включения изучения MAC-адресов на физическом порту или VLAN. Используйте форму **no**, чтобы отключить данную функцию.

mac-address-table learning interface {vlan VLAN-ID [, | -] | INTERFACE-ID [, | -]}
no mac-address-table learning interface {vlan VLAN-ID [, | -] | INTERFACE-ID [, | -]}

Параметры

vlan VLAN-ID	Укажите VLAN ID, который необходимо сконфигурировать.
,	(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.
INTERFACE-ID	Укажите интерфейс физического порта, который необходимо сконфигурировать.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить/отключить изучение MAC-адресов на физическом порту или VLAN.

Ниже описаны правила изучения MAC-адресов на интерфейсах VLAN:

На всех VLAN коммутатора при создании по умолчанию всегда включено изучение MAC-адресов. При удалении VLAN функция изучения MAC-адресов вернется к настройкам по умолчанию.

Изучение MAC-адресов можно настроить только на существующей VLAN.

При отключении изучения MAC-адресов на VLAN, данная функция будет приостановлена на всех портах, принадлежащих данной VLAN.

При отключении изучения MAC-адресов на Voice VLAN / Surveillance VLAN, данная функция будет работать неправильно на основании изучения MAC-адресов.

Отключение изучения MAC-адресов на VLAN приведет к неправильной работе Asymmetric VLAN на связанных VLAN.

Отключение распознавания MAC-адресов на Private VLAN приведет к неправильной работе Private VLAN.

Remote-Span (RSPAN) VLAN обладают более высоким приоритетом, при этом на RSPAN VLAN изучение MAC-адресов всегда отключено. При удалении RSPAN VLAN будет включено изучение сконфигурированных MAC-адресов.

Изучение MAC-адресов для модулей безопасности, таких как Port Security, 802.1x, MAC-based Access Control, Web-based Access Control и IMPV, обладает более высоким приоритетом. Если изучение MAC-адресов отключить на VLAN, включающей secure port, данная функция продолжит работу. Если все secure ports на VLAN отключены, будет включено изучение сконфигурированных MAC-адресов.

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)#
```

37-5 mac-address-table notification change

Данная команда используется для включения/настройки функции уведомлений о MAC-адресах. Используйте форму **no**, чтобы отключить функцию или вернуться к настройкам по умолчанию.

mac-address-table notification change [interval SECONDS | history-size VALUE | trap-type {with-vlanid | without-vlanid}]
no mac-address-table notification change [interval | history-size | trap-type]

Параметры

interval SECONDS	(Опционально) Укажите интервал отправки трап-сообщений о MAC-адресах в диапазоне от 1 до 2147483647 секунд. Значение по умолчанию – 1 секунда.
history-size VALUE	(Опционально) Укажите максимальное количество записей в таблице истории уведомлений. Доступный диапазон значений: от 0 до 500 записей. Значение по умолчанию – 1 запись.
trap-type	(Опционально) Укажите, будет ли информация о трапе содержать VLAN ID.

По умолчанию

Уведомления о MAC-адресах отключены.
 Интервал отправки трапов по умолчанию – 1 секунда.
 Количество записей в таблице истории уведомлений по умолчанию – 1.
 Тип трапа по умолчанию – without-vlanid.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

При распознавании или удалении коммутатором MAC-адреса соответствующее уведомление может быть отправлено в таблицу истории уведомлений, а затем на SNMP-сервер, если запущена команда **snmp-server enable traps mac-notification change**. В таблице истории уведомлений хранятся распознанные или удаленные MAC-адреса тех интерфейсов, для которых включены трапы. Для групповых адресов события не генерируются.

Пример

В данном примере показано, как включить уведомления об изменении MAC-адреса и установить интервал 10 секунд, а лимит по количеству записей в истории – 500.

```
Switch# configure terminal
Switch(config)# mac-address-table notification change
Switch(config)# mac-address-table notification change interval 10
Switch(config)# mac-address-table notification change history-size 500
Switch(config)#
```

37-6 mac-address-table static

Данная команда используется для добавления статического адреса в таблицу MAC-адресов. Используйте форму **no**, чтобы удалить запись из таблицы.

mac-address-table static MAC-ADDR vlan VLAN-ID {interface INTERFACE-ID [, | -] | drop}
no mac-address-table static {all | MAC-ADDR vlan VLAN-ID [interface INTERFACE-ID] [, | -]}

Параметры

MAC-ADDR	Укажите индивидуальный или групповой MAC-адрес. Пакеты с адресом назначения (destination), соответствующим данному MAC-адресу, полученные указанной VLAN, будут направлены на указанный интерфейс.
vlan VLAN-ID	Укажите VLAN записи в диапазоне от 1 до 4094.
interface INTERFACE-ID	Укажите порты продвижения кадров.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
drop	Укажите, чтобы отбросить кадры, отправленные с указанного MAC-адреса / на указанный MAC-адрес на обозначенной VLAN.
all	Укажите, чтобы удалить все записи статических MAC-адресов.

По умолчанию

По умолчанию сконфигурированные статические адреса отсутствуют.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Для записи индивидуального MAC-адреса можно указать только один интерфейс. Для записи группового MAC-адреса можно указать несколько интерфейсов. Чтобы удалить запись индивидуального MAC-адреса, interface ID указывать не нужно. При удалении записи группового MAC-адреса будет удален только тот интерфейс, ID которого указан. Если interface ID не указан, будет удалена вся запись группового MAC-адреса. Параметр drop может быть применен только для записи индивидуального MAC-адреса.

Пример

В данном примере показано, как добавить статический адрес C2:F3:22:0A:12:F4 в таблицу MAC-адресов. Если пакет с MAC-адресом назначения C2:F3:22:0A:12:F4 получен на VLAN 4, он будет направлен на интерфейс Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# mac-address-table static C2:F3:22:0A:12:F4 vlan 4 interface ethernet 1/0/1
Switch(config)#
```

37-7 multicast filtering-mode (Interface)

Данная команда используется для настройки способа обработки групповых пакетов на интерфейсе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
multicast filtering-mode {forward-all | forward-unregistered | filter-unregistered}
no multicast filtering-mode
```

Параметры

forward-all	Укажите, чтобы распространить все групповые пакеты на основании VLAN-домена.
forward-unregistered	Укажите, чтобы направить зарегистрированные групповые пакеты на основании таблицы переадресации и распространить все незарегистрированные групповые пакеты на основании VLAN-домена.
filter-unregistered	Укажите, чтобы направить зарегистрированные пакеты на основании таблицы переадресации и отфильтровать все незарегистрированные групповые пакеты.

По умолчанию

Параметр по умолчанию – **forward-unregistered**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данный режим фильтрации применим только к групповым пакетам, предназначенным для адресов, незарезервированных для групповых адресов.

Пример

В данном примере показано, как установить режим фильтрации групповых пакетов на VLAN 100, чтобы отфильтровать незарегистрированные адреса.

```
Switch# configure terminal
Switch(config)# vlan 100
Switch(config-vlan)# multicast filtering-mode filter-unregistered
Switch(config-vlan)#
```


37-8 show mac-address-table

Данная команда используется для отображения записи указанного MAC-адреса или записей MAC-адреса для указанного интерфейса/VLAN.

```
show mac-address-table [dynamic | static] [address MAC-ADDR | interface [INTERFACE-ID |vlan VLAN-ID]
```

Параметры

dynamic	(Опционально) Укажите, чтобы отобразить только записи таблицы динамических MAC-адресов.
static	(Опционально) Укажите, чтобы отобразить только записи таблицы статических MAC-адресов.
address MAC-ADDR	(Опционально) Укажите 48-битный MAC-адрес.
interface INTERFACE-ID	(Опционально) Укажите, чтобы отобразить информацию для указанного интерфейса (физического порта или port-channel).
vlan VLAN-ID	(Опционально) Укажите VLAN ID в диапазоне от 1 до 4094.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

При указании параметра **interface** будет отображена индивидуальная запись, чей интерфейс передачи соответствует указанному интерфейсу.

Пример

В данном примере показано, как отобразить все записи таблицы MAC-адресов для MAC-адреса 00-23-7D-BC-08-44.

```
Switch#show mac-address-table address 00-23-7D-BC-08-44
```

VLAN	MAC Address	Type	Ports
1	00-23-7D-BC-08-44	Dynamic	eth1/0/5

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	F0-7D-68-34-00-10	Static	CPU

Total Entries: 1

```
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	00-23-7D-BC-08-44	Dynamic	eth1/0/5
1	00-23-7D-BC-2E-18	Dynamic	eth1/0/1
1	00-FF-47-77-70-B8	Dynamic	eth1/0/5
1	10-BF-48-D6-E2-E2	Dynamic	eth1/0/5
1	24-24-0E-E5-96-DE	Dynamic	eth1/0/5
1	40-B8-37-B1-06-9A	Dynamic	eth1/0/5
1	5C-33-8E-43-B3-68	Dynamic	eth1/0/5
1	CC-B2-55-8B-27-79	Dynamic	eth1/0/5
1	F0-7D-68-34-00-10	Static	CPU

Total Entries: 9

```
Switch#
```

37-9 show mac-address-table aging-time

Данная команда используется для отображения времени устаревания MAC-адресов в таблице.

```
show mac-address-table aging-time
```

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить время устаревания MAC-адресов в таблице.

Пример

В данном примере показано, как отобразить время устаревания MAC-адресов в таблице.

```
Switch# show mac-address-table aging-time
Aging Time is 300 seconds
Switch#
```

37-10 show mac-address-table learning

Данная команда используется для отображения статуса изучения MAC-адресов.

show mac-address-table learning interface [vlan [VLAN-ID [, | -]] | INTERFACE-ID [, | -]]

Параметры

<i>VLAN-ID</i>	(Опционально) Укажите VLAN ID, который необходимо отобразить. Если ID не указан, будут отображены все VLAN.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
<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

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Если не указаны дополнительные параметры, будут отображены все физические порты.

Пример

В данном примере показано, как отобразить статус изучения MAC-адресов на всех физических портах от 1 до 10.

```
Switch#show mac-address-table learning interface ethernet 1/0/1-10

Port                State
-----
eth1/0/1            Enabled
eth1/0/2            Enabled
eth1/0/3            Enabled
eth1/0/4            Enabled
eth1/0/5            Enabled
eth1/0/6            Enabled
eth1/0/7            Enabled
eth1/0/8            Enabled
eth1/0/9            Enabled
eth1/0/10           Enabled

Switch#
```

37-11 show mac-address-table notification change

Данная команда используется для отображения настроек уведомлений о MAC-адресах или истории уведомлений.

show mac-address-table notification change [interface [INTERFACE-ID] | history]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите интерфейс, который необходимо отобразить.
history	(Опционально) Укажите, чтобы отобразить историю уведомлений об изменении MAC-адреса.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Если не указаны дополнительные параметры, будут отображены общие настройки. Используйте параметр **interface**, чтобы отобразить информацию обо всех интерфейсах. Чтобы отобразить конкретный интерфейс, введите его ID.

Пример

В данном примере показано, как отобразить настройки уведомлений об изменении MAC-адреса на всех интерфейсах.

```
Switch#show mac-address-table notification change interface
```

Interface	Added Trap	Removed Trap
eth1/0/1	Disabled	Disabled
eth1/0/2	Disabled	Disabled
eth1/0/3	Disabled	Disabled
eth1/0/4	Disabled	Disabled
eth1/0/5	Disabled	Disabled
eth1/0/6	Disabled	Disabled
eth1/0/7	Disabled	Disabled
eth1/0/8	Disabled	Disabled
eth1/0/9	Disabled	Disabled
eth1/0/10	Disabled	Disabled
eth1/0/11	Disabled	Disabled
eth1/0/12	Disabled	Disabled
eth1/0/13	Disabled	Disabled
eth1/0/14	Disabled	Disabled
eth1/0/15	Disabled	Disabled
eth1/0/16	Disabled	Disabled
eth1/0/17	Disabled	Disabled
eth1/0/18	Disabled	Disabled
eth1/0/19	Disabled	Disabled
eth1/0/20	Disabled	Disabled

```
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

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
Trap Type: Without VID
Switch#
```

В данном примере показано, как отобразить историю уведомлений о MAC-адресах.

```
Switch# show mac-address-table notification change history
History Index: 1
Operation:ADD Vlan: 1 MAC Address: 00-f8-d0-12-34-56 eth1/0/1
History Index: 2
Operation:DEL Vlan: 1 MAC Address: 00-f8-d0-00-00-01 eth1/0/1
History Index: 3
Operation:DEL Vlan: 1 MAC Address: 00-f8-d0-00-00-02 eth1/0/1
Switch#
```

37-12 show multicast filtering-mode

Данная команда используется для отображения режима фильтрации при обработке групповых пакетов, полученных на интерфейсе.

show multicast filtering-mode [interface *INTERFACE-ID*]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите VLAN, которую необходимо отобразить.
--------------------------------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Пример

В данном примере показано, как отобразить настройки режима фильтрации групповых пакетов для всех VLAN.

```
Switch#show multicast filtering-mode

Interface                               Layer 2 Multicast Filtering Mode
-----                               -
default                                 forward-unregistered

Total Entries: 1

Switch#
```

37-13 snmp-server enable traps mac-notification change

Данная команда используется для включения отправки SNMP Trap об уведомлениях MAC. Используйте форму **no**, чтобы отключить данную функцию.

```
snmp-server enable traps mac-notification change
no snmp-server enable traps mac-notification change
```

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить 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)#
```

37-14 snmp trap mac-notification change

Данная команда используется для включения уведомлений об изменении MAC-адреса на указанном интерфейсе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

snmp trap mac-notification change {added | removed}
no snmp trap mac-notification change {added | removed}

Параметры

added	Укажите, чтобы включить уведомления об изменении MAC-адреса при добавлении MAC-адреса на интерфейс.
removed	Укажите, чтобы включить уведомления об изменении MAC-адреса при удалении MAC-адреса с интерфейса.

По умолчанию

По умолчанию отправка трапов о добавлении/удалении адреса отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Даже если при помощи команды **snmp trap mac-notification change** на интерфейсе включена отправка уведомлений, уведомления будут отправлены в таблицу истории только при использовании команды **mac-address-table notification change**.

Пример

В данном примере показано, как включить уведомления о добавлении MAC-адреса на интерфейсе Ethernet 1/0/2.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# snmp trap mac-notification change added
Switch(config-if)#
```


38. Команды Filter NetBIOS

38-1 deny netbios

Данная команда используется для блокировки пакетов NetBIOS на указанном интерфейсе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
deny netbios
no deny netbios
```

Параметры

Нет

По умолчанию

По умолчанию пакеты NetBIOS разрешены.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы заблокировать/разрешить пакеты NetBIOS на физических портах.

Пример

В данном примере показано, как заблокировать пакеты NetBIOS на порту Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#deny netbios
Switch(config-if)#
```

38-2 deny extensive-netbios

Данная команда используется для блокировки пакетов NetBIOS в кадрах 802.3 на указанном интерфейсе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
deny extensive-netbios
no deny extensive-netbios
```

Параметры

Нет

По умолчанию

По умолчанию пакеты NetBIOS в кадрах 802.3 разрешены.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы заблокировать/разрешить пакеты NetBIOS в кадрах 802.3 на физических портах.

Пример

В данном примере показано, как заблокировать пакеты NetBIOS в кадрах 802.3 на порту Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#deny extensive-netbios
Switch(config-if)#
```

39. Команды GARP VLAN Registration Protocol (GVRP)

39-1 clear gvrp statistics

Данная команда используется для удаления статистики GVRP на порту.

```
clear gvrp statistics {all | interface INTERFACE-ID [, | -]}
```

Параметры

all	Укажите, чтобы обнулить счетчики статистики GVRP, ассоциированные со всеми интерфейсами.
interface <i>INTERFACE-ID</i>	Укажите интерфейсы, которые необходимо сконфигурировать.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы обнулить счетчики GVRP.

Пример

В данном примере показано, как удалить статистику для всех интерфейсов.

```
Switch# clear gvrp statistics all
Switch#
```

39-2 gvrp global

Данная команда используется для глобального включения функции GVRP. Используйте форму **no**, чтобы глобально отключить функцию GVRP.

```
gvrp global
no gvrp global
```

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

GVRP можно включить как глобально, так и на отдельном порту.

Пример

В данном примере показано, как включить GVRP-протокол глобально.

```
Switch# configure terminal
Switch(config)# gvrp global
Switch(config)#
```

39-3 gvrp enable

Данная команда используется для включения функции GVRP на порту. Используйте форму **no**, чтобы отключить данную функцию.

```
gvrp enable
no gvrp enable
```

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки физических портов и port-channel в режимах Hybrid Mode и Trunk Mode. Если для GVRP включена функция Layer 2 Protocol Tunnel, применение команды невозможно.

Пример

В данном примере показано, как включить функцию GVRP на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# gvrp enable
Switch(config-if)#
```

39-4 gvrp advertise

Используйте данную команду, чтобы указать VLAN, для которых разрешено анонсирование при помощи GVRP-протокола. Используйте форму **no**, чтобы отключить данную функцию.

```
gvrp advertise {all | [add | remove] VLAN-ID [, | -]}
no gvrp advertise
```

Параметры

all	Укажите, чтобы включить анонсирование для всех VLAN на интерфейсе.
add	(Опционально) Укажите одну или несколько VLAN, которые необходимо добавить в список анонсирования.
remove	(Опционально) Укажите одну или несколько VLAN, которые необходимо удалить из списка анонсирования.
<i>VLAN-ID</i>	Укажите VLAN ID, который необходимо добавить в список анонсирования или удалить из данного списка. Если не указан параметр add или remove , список указанных VLAN заменит текущий список анонсирования. Доступный диапазон значений: от 1 до 4094.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию анонсирование VLAN отключено.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки физических портов и port-channel в режимах Hybrid Mode и Trunk Mode. Используйте команду **gvrp advertise**, чтобы включить функцию анонсирования GVRP для указанных VLAN на указанном интерфейсе. Предварительно необходимо включить GVRP.

Пример

В данном примере показано, как включить функцию анонсирования для VLAN 1000 на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# gvrp advertise 1000
Switch(config-if)#
```

39-5 gvrp vlan create

Данная команда используется для того, чтобы включить создание Dynamic VLAN. Используйте форму **no**, чтобы отключить данную функцию.

```
gvrp vlan create
no gvrp vlan create
```

Параметры

Нет

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если данная функция включена и на порту обнаружено новое членство VLAN, но при этом данной VLAN не существует, VLAN будет создана автоматически. Иначе изученная VLAN не будет создана.

Пример

В данном примере показано, как включить создание dynamic VLAN, зарегистрированных с помощью GVRP-протокола.

```
Switch# configure terminal
Switch(config)# gvrp vlan create
Switch(config)#
```

39-6 gvrp forbidden

Данная команда используется для указания порта, которому запрещено быть членом обозначенной VLAN. Используйте форму **no**, чтобы удалить статус запрещенного члена всех VLAN для порта.

```
gvrp forbidden {all | [add | remove] VLAN-ID [, | -]}
no gvrp forbidden
```

Параметры

all	Укажите, чтобы запретить на интерфейсе все VLAN, кроме VLAN 1.
add	(Опционально) Укажите одну или несколько VLAN, которые необходимо добавить в список запрещенных VLAN.
remove	(Опционально) Укажите одну или несколько VLAN, которые необходимо удалить из списка запрещенных VLAN.
<i>VLAN-ID</i>	Укажите список запрещенных VLAN. Если не указан параметр add или remove , список данных VLAN заменит текущий список запрещенных VLAN. Доступный диапазон значений: от 2 до 4094.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию ни одна из VLAN не запрещена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки физических портов и port-channel в режимах Hybrid Mode и Trunk Mode. Порт, указанный в качестве запрещенного порта VLAN, не может стать членом VLAN при помощи GVRP. VLAN, обозначенная при помощи данной команды, может не существовать.

Команда влияет только на работу GVRP, при этом GVRP необходимо предварительно включить.

Пример

В данном примере показано, как настроить порт ethernet 1/0/1 в качестве запрещенного порта для VLAN 1000 при помощи GVRP.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# gvrp forbidden 1000
Switch(config-if)#
```

39-7 gvrp timer

Данная команда используется для настройки значения таймера GVRP на порту. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
gvrp timer [join TIMER-VALUE] [leave TIMER-VALUE] [leave-all TIMER-VALUE]
no gvrp timer [join] [leave] [leave-all]
```

Параметры

join	(Опционально) Установите значение таймера для входа в группу. Единицы измерения – сотые доли секунды.
leave	(Опционально) Установите значение таймера для выхода из группы. Единицы измерения – сотые доли секунды.
leave-all	(Опционально) Установите значение таймера для выхода из всех групп. Единицы измерения – сотые доли секунды.
<i>TIMER-VALUE</i>	(Опционально) Установите значение таймера. Доступный диапазон значений: от 10 до 10000 сотых долей секунды.

По умолчанию

Join: 20
Leave: 60
Leave-all: 1000

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить значение таймера GVRP на порту.

Пример

В данном примере показано, как настроить значение таймера для выхода из всех групп на порту Ethernet 1/0/1. Установленное значение – 500 сотых долей секунды.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# gvrp timer leave-all 500
Switch(config-if)#
```


39-8 gvrp nni-bpdu-address

Данная команда используется для настройки адреса GVRP BPDU на сайте поставщика услуг. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
gvrp nni-bpdu-address {dot1d | dot1ad}  
no gvrp nni-bpdu-address
```

Параметры

dot1d	Укажите, чтобы назначить адрес GVRP 802.1d 01:80:C2:00:00:21 в качестве адреса протокола GVRP BPDU.
dot1ad	Укажите, чтобы назначить адрес GVRP 802.1ad 01:80:C2:00:00:0D в качестве адреса протокола GVRP BPDU.

По умолчанию

Адрес GVRP по умолчанию – 802.1d.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Обычно в качестве адреса GVRP BPDU используется адрес Dot1d GVRP. Данная команда используется для назначения адреса Dot1d или Dot1ad GVRP в качестве адреса GVRP BPDU на сайте поставщика услуг. Команда доступна только на trunk-портах VLAN, которые действуют в качестве портов NNI на сайте поставщика услуг.

Пример

В данном примере показано, как настроить адрес GVRP BPDU на сайте поставщика услуг. Назначенный адрес – dot1d.

```
Switch# configure terminal  
Switch(config)# gvrp nni-bpdu-address dot1d  
Switch(config)#
```

39-9 show gvrp configuration

Данная команда используется для отображения настроек GVRP.

```
show gvrp configuration [interface [INTERFACE-ID [, | -]]]
```

Параметры

interface	(Опционально) Укажите, чтобы отобразить настройки GVRP для интерфейса. Если interface ID не указан, будут отображены настройки всех интерфейсов.
<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

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить настройки GVRP. Если не указан ни один из параметров, будут отображены глобальные настройки GVRP.

Пример

В данном примере показано, как отобразить глобальные настройки GVRP.

```
Switch# show gvrp configuration

Global GVRP State      : Enabled
Dynamic VLAN Creation  : Disabled
NNI BPDU Address      : Dot1d

Switch#
```

В данном примере показано, как отобразить настройки GVRP на интерфейсах Ethernet 1/0/5 и Ethernet 1/0/6.

```

Switch# show gvrp configuration interface ethernet 1/0/5-1/0/6

ethernet 1/0/5
GVRP Status      : Enabled
Join Time        : 20 centiseconds
Leave Time        : 60 centiseconds
Leave-All Time    : 1000 centiseconds
Advertise VLAN   : 1-4094
Forbidden VLAN   : 3-5

ethernet 1/0/6
GVRP Status      : Enabled
Join Time        : 20 centiseconds
Leave Time        : 60 centiseconds
Leave-All Time    : 1000 centiseconds
Advertise VLAN   : 1-3
Forbidden VLAN   : 5-8

Switch#

```

39-10 show gvrp statistics

Данная команда используется для отображения статистики GVRP на порту.

show gvrp statistics [interface *INTERFACE-ID* [, | -]]

Параметры

interface <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

User EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить порты, на которых включен режим GVRP.

Пример

В данном примере показано, как отобразить статистику GVRP для интерфейсов Ethernet 1/0/5 и Ethernet 1/0/6.

```
Switch#show gvrp statistics interface ethernet 1/0/5-1/0/6
```

Interface	JoinEmpty	JoinIn	LeaveEmpty	LeaveIn	LeaveAll	Empty
eth1/0/5	RX 0	0	0	0	0	0
	TX 4294967296	4294967296	4294967296	4294967296	4294967296	4294967296
eth1/0/6	RX 0	0	0	0	0	0
	TX 0	0	0	0	0	0

```
Switch#
```

40. Команды Gratuitous ARP

40-1 ip arp gratuitous

Данная команда используется для включения изучения пакетов Gratuitous ARP в таблице ARP-кэша. Используйте форму **no**, чтобы отключить ARP control.

```
ip arp gratuitous
no ip arp gratuitous
```

Параметры

Нет

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

По умолчанию система изучает пакеты Gratuitous ARP в таблице ARP-кэша.

Пример

В данном примере показано, как отключить изучение пакетов Gratuitous ARP Request.

```
Switch# configure terminal
Switch(config)# no ip arp gratuitous
Switch(config)#
```

40-2 ip gratuitous-arps

Данная команда используется для того, чтобы включить передачу пакетов Gratuitous ARP Request. Используйте форму **no**, чтобы отключить передачу.

```
ip gratuitous-arps [dad-reply]
no ip gratuitous-arps [dad-reply]
```

Параметры

dad-reply	(Опционально) Укажите, будет ли система высылать ответный пакет Gratuitous ARP Request с Broadcast DA при получении пакета Gratuitous ARP Request и обнаружении
------------------	---

дублированного IP-адреса.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Пакет Gratuitous ARP Request – это пакет запроса ARP, где IP-адрес источника (source) и IP-адрес назначения (destination) являются IP-адресом передающего устройства, а MAC-адрес назначения – широковещательным адресом.

Устройство использует пакет Gratuitous ARP Request, чтобы определить, дублирован ли IP-адрес другими узлами, или выполнить предварительную загрузку / перенастроить конфигурацию записи ARP-кэша узлов, подключенных к интерфейсу.

Используйте команду **ip gratuitous-arps**, чтобы включить передачу запроса Gratuitous ARP. Устройство вышлет пакет, если IP-интерфейс в состоянии link-up или если IP-адрес интерфейса сконфигурирован/изменен.

Используйте команду **ip gratuitous-arps dad-reply**, чтобы включить передачу запросов Gratuitous ARP. Устройство вышлет пакет при обнаружении дублированного IP-адреса.

Пример

В данном примере показано, как отправлять сообщения Gratuitous ARP.

```
Switch# configure terminal
Switch(config)# ip gratuitous-arps dad-reply
Switch(config)#
```

40-3 arp gratuitous-send interval

Данная команда используется для установки интервала отправки сообщений Gratuitous ARP Request на интерфейс. Используйте форму **no**, чтобы отключить данную функцию.

```
arp gratuitous-send interval SECONDS
no arp gratuitous-send
```

Параметры

<i>SECONDS</i>	Укажите временной интервал для отправки сообщений с Gratuitous ARP Request. Доступный диапазон значений: от 0 до 3600. Если указан 0, данная опция отключена.
----------------	---

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если интерфейс коммутатора используется в качестве шлюза для конечных устройств и у данных устройств наблюдается поведение ложного шлюза, администратор может настроить регулярную отправку сообщений с Gratuitous ARP Request на данном интерфейсе для уведомления о том, что коммутатор является подлинным шлюзом.

Пример

В данном примере показано, как включить отправку сообщений Gratuitous ARP.

```
Switch# configure terminal
Switch(config)# ip gratuitous-arps
Switch(config)# interface vlan 100
Switch(config-if)# arp gratuitous-send interval 1
Switch(config-if)#
```

40-4 snmp-server enable traps gratuitous-arp

Данная команда используется для включения отправки SNMP-уведомлений об обнаружении дублированного IP-адреса Gratuitous ARP. Используйте форму **no**, чтобы отключить данную функцию.

```
snmp-server enable traps gratuitous-arp
no snmp-server enable traps gratuitous-arp
```

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения/отключения отправки SNMP-уведомлений об обнаружении дублированного IP-адреса Gratuitous ARP.

Пример

В данном примере показано, как включить отставку SNMP-уведомлений об обнаружении дублированного IP-адреса Gratuitous ARP.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps gratuitous-arp
Switch(config)#
```


41. Команды управления интерфейсом

41-1 clear counters

Данная команда используется для сброса всех счетчиков для указанных интерфейсов.

```
clear counters {all | interface INTERFACE-ID [, | -]}
```

Параметры

all	Укажите, если необходимо сбросить счетчики для всех интерфейсов.
interface <i>INTERFACE-ID</i>	Укажите настраиваемые интерфейсы. Интерфейсами могут считаться физические порты, порт управления ООВ, port-channel или интерфейсы VLAN 2-го уровня.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для сброса счетчиков для интерфейса физического порта.

Пример

В данном примере показан процесс сброса счетчиков для Ethernet 1/0/1.

```
Switch# clear counters interface ethernet 1/0/1
Switch#
```

42-2 description

Данная команда используется для добавления описания для интерфейса. При использовании формы **no** команда удалит описание.

```
description STRING
no description
```

Параметры

<i>STRING</i>	Описание для интерфейса. Максимально допустимое количество символов – 64.
---------------	---

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Указанное описание соответствует объекту MIB «ifAlias», определенному в RFC 2233.

Пример

В данном примере показано, как добавить описание «Physical Port 10» на интерфейс Ethernet 1/0/10.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/10
Switch(config-if)# description Physical Port 10
Switch(config-if)#
```

41-3 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>	Укажите идентификатор интерфейса (Interface ID). ID интерфейса состоит из типа интерфейса и номера интерфейса без пробелов между ними.
---------------------	--

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для входа в режим Interface Configuration Mode для определенного интерфейса. ID интерфейса состоит из типа интерфейса и номера интерфейса без пробелов между ними. Поддерживаются и могут использоваться следующие ключевые слова:

- **Ethernet** – физический порт Ethernet-коммутатора любой среды
- **L2vlan** – виртуальный LAN-интерфейс второго уровня IEEE 802.1Q
- **Loopback** – программный интерфейс, который всегда находится в рабочем состоянии
- **mgmt** – интерфейс Ethernet, используемый для управления портом Out-of-Band
- **Null** – интерфейс null
- **Port-channel** – агрегированный интерфейс port-channel
- **Tunnel** – виртуальный интерфейс, используемый для туннелирования
- **Vlan** – интерфейс VLAN

Формат номера интерфейса зависит от типа интерфейса.

Для интерфейсов физических портов пользователь не может войти в интерфейс, если порт коммутатора не существует. Интерфейс физического порта не может быть удален командой **no**.

Используйте команду **interface Vlan** для создания интерфейса 3 уровня. Используйте команду **vlan** в режиме Global Configuration Mode, чтобы создать VLAN перед созданием интерфейса 3 уровня. Используйте команду **no interface Vlan**, чтобы удалить интерфейс 3 уровня.

Интерфейс port-channel автоматически создается, когда команда **channel-group** настроена для интерфейса физического порта. Интерфейс port-channel будет удален автоматически, если для команды **channel-group** не будет настроен интерфейс физического порта. Используйте команду **nointerface Port-channel**, чтобы удалить port-channel.

Для интерфейса null поддерживается интерфейс null0, и он не может быть удален.

Для интерфейсов loopback или tunnel команда **interface** используется для создания интерфейса или изменения настроек интерфейса. При использовании формы **no** команда удалит интерфейс.

Режимы интерфейсов **L2vlan** и **L2vc** используются только для добавления описания к существующим L2VLAN и L2 Virtual circuit. Команды **interface l2vlan** и **interface l2vc** не создают новые интерфейсы, и никакие формы по данным команд не удаляют существующие интерфейсы.

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)#
```

В данном примере показано, как добавить интерфейс loopback 2 и войти в режим Interface Configuration Mode.

```
Switch# configure terminal
Switch(config)# interface loopback2
Switch (config-if)#
```

В данном примере показано, как удалить интерфейс loopback 2.

```
Switch# configure terminal
Switch(config)# no interface loopback2
Switch (config)#
```

41-4 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>	Укажите ID интерфейса. ID интерфейса состоит из типа интерфейса и номера интерфейса без пробелов между ними.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для входа в режим Interface Configuration Mode для указанного диапазона интерфейсов. Команды, введенные в режиме Interface Range Mode, применяются ко всем интерфейсам в диапазоне.

Пример

В данном примере показано, как войти в режим Interface Configuration Mode для диапазона портов от 2/0/1 до 2/0/5, а также для порта 3/0/3.

```
Switch# configure terminal
Switch(config)# interface range Ethernet 2/0/1-5, 3/0/3
Switch(config-if-range)#
```

41-5 show counters

Данная команда используется для отображения информации об интерфейсе.

show counters [interface *INTERFACE-ID*]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите необходимый интерфейс: физический порт, port-channel или VLAN. Если интерфейс не указан, будут отображаться счетчики для всех интерфейсов.
--------------------------------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения статистики счетчиков для интерфейса. Следующие пункты предоставляют подробную информацию об отображении параметров данной команды:

- **max-rcv-frame-size:** максимальный размер Ethernet-кадра, определенный в командах **Jumbo**
- **Frame.** Диапазон доступных значений – от 64 до 12288 байт.

Пример

В данном примере показано, как включить отображение счетчиков для Ethernet 1/0/1.

```
Switch#show counters interface ethernet 1/0/1
```

```
eth1/0/1 counters
rxHCTotalPkts           : 67004
txHCTotalPkts           : 63918
rxHCUnicastPkts        : 66026
txHCUnicastPkts        : 46199
rxHCMulticastPkts      : 383
txHCMulticastPkts      : 9848
rxHCBroadcastPkts     : 595
txHCBroadcastPkts     : 7871
rxHCOctets              : 14339916
txHCOctets              : 13420831
rxHCPkt64Octets        : 45325
rxHCPkt65to127Octets   : 1058
rxHCPkt128to255Octets  : 0
rxHCPkt256to511Octets  : 4705
rxHCPkt512to1023Octets : 15916
rxHCPkt1024to1518Octets : 0
rxHCPkt1519to1522Octets : 0
rxHCPkt1519to2047Octets : 0
rxHCPkt2048to4095Octets : 0
rxHCPkt4096to9216Octets : 0
txHCPkt64Octets        : 6347
txHCPkt65to127Octets   : 21566
```

```

txHCPkt128to255Octets      : 27683
txHCPkt256to511Octets     : 5822
txHCPkt512to1023Octets    : 270
txHCPkt1024to1518Octets   : 2230
txHCPkt1519to1522Octets   : 0
txHCPkt1519to2047Octets   : 0
txHCPkt2048to4095Octets   : 0
txHCPkt4096to9216Octets   : 0

rxCRCAlignErrors          : 0
rxUndersizedPkts         : 0
rxFragmentPkts           : 0
rxSymbolErrors           : 0
rxDropPkts               : 0

txCollisions              : 0
ifInErrors                 : 0
ifOutErrors                : 0
ifInDiscards              : 0
ifOutDiscards             : 0
txDelayExceededDiscards   : 0
txCRC                     : 0

dot3StatsSingleColFrames  : 0
dot3StatsMultiColFrames   : 0
dot3StatsDeferredTransmissions : 0
dot3StatsLateCollisions   : 0
dot3StatsExcessiveCollisions : 0
dot3StatsInternalMacTransmitErrors : 0
dot3StatsFrameTooLongs    : 0

linkChange                 : 1

Switch#
    
```

Отображаемые параметры

rxHCTotalPkts	Счетчик принятых пакетов. Возрастает с каждым принятым пакетом (включая поврежденные пакеты, все одноадресные, широковещательные и многоадресные пакеты и пакеты управления MAC).
txHCTotalPkts	Счетчик переданных пакетов. Возрастает с каждым переданным пакетом (включая поврежденные пакеты, все одноадресные, широковещательные и многоадресные пакеты и пакеты управления MAC).
rxHCUnicastPkts	Счетчик принятых пакетов одноадресной рассылки. Возрастает с каждым успешно принятым пакетом одноадресной рассылки.
txHCUnicastPkts	Счетчик переданных пакетов одноадресной рассылки. Возрастает с каждым успешно переданным пакетом одноадресной рассылки.

rxHCMulticastPkts	Счетчик принятых пакетов многоадресной рассылки. Возрастает с каждым успешно принятым пакетом многоадресной рассылки, исключая пакеты управления MAC.
txHCMulticastPkts	Счетчик переданных пакетов многоадресной рассылки. Возрастает с каждым успешно переданным пакетом многоадресной рассылки, исключая пакеты управления MAC.
rxHCBroadcastPkts	Счетчик принятых пакетов широковещательной рассылки. Возрастает с каждым успешно принятым пакетом широковещательной рассылки.
txHCBroadcastPkts	Счетчик переданных пакетов широковещательной рассылки. Возрастает с каждым успешно переданным пакетом широковещательной рассылки.
rxHCOctets	Счетчик принятых байтов. Возрастает с подсчетом байтов принятых пакетов, исключая поврежденные пакеты. (Исключая биты кадров, но включая байты FCS) Примечание: Для усеченного пакета счетчик учитывает только размер max-rcv-frame.
txHCOctets	Счетчик переданных байтов. Возрастает с подсчетом байтов переданных пакетов, исключая поврежденные пакеты. (Исключая биты кадров, но включая байты FCS)
rxHCPkt64Octets	Счетчик принятых 64-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), до 64 байт включительно (исключая биты кадров, но включая байты FCS).
rxHCPkt65to127Octets	Счетчик принятых 64 – 127-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 65 до 127 байт включительно (исключая биты кадров, но включая байты FCS).
rxHCPkt128to255Octets	Счетчик принятых 128 – 255-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 128 до 255 байт включительно (исключая биты кадров, но включая байты FCS).
rxHCPkt256to511Octets	Счетчик принятых 256 – 511-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 256 до 511 байт включительно (исключая биты кадров, но включая байты FCS).
rxHCPkt512to1023Octets	Счетчик принятых 512 – 1023-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 512 до 1023 байт включительно (исключая биты кадров, но включая байты FCS).
rxHCPkt1024to1518Octets	Счетчик принятых 1024 – 1518-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type),

	от 1024 до 1518 байтвключительно (исключая биты кадров, но включая байты FCS).
rxHCPkt1519to1522Octets	Счетчик принятых допустимых 1519 – 1522-байтовых кадров VLAN. Возрастает с каждым допустимым принятым кадром VLAN (исключая FCS, Symbol, ошибка Truncated), от 1519 до 1522 байт включительно (исключая биты кадров, но включая байты FCS). Подсчитываются как одиночные, так и дваждытегированные кадры.
rxHCPkt1519to2047Octets	Счетчик принятых 1519 – 2047-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 1519 до 2047 байтвключительно (исключая биты кадров, но включая байты FCS).
rxHCPkt2048to4095Octets	Счетчик принятых 2048 – 4095-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 2048 до 4095 байтвключительно (исключая биты кадров, но включая байты FCS).
rxHCPkt4096to9216Octets	Счетчик принятых 4096 – 9216-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 4096 до 9216 байтвключительно (исключая биты кадров, но включая байты FCS).
rxHCPkt9217to16383Octets	Счетчик принятых 9217 – 16383-байтовых кадров. Возрастает с каждым допустимым и поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 9217 до 16383 байтвключительно (исключая биты кадров, но включая байты FCS).
txHCPkt64Octets	Счетчик переданных 64-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), до 64 байт включительно (исключая биты кадров, но включая байты FCS).
txHCPkt65to127Octets	Счетчик переданных 65 – 127-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 65 до 127 байт включительно (исключая биты кадров, но включая байты FCS).
txHCPkt128to255Octets	Счетчик переданных 128 – 255-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 128 до 255 байт включительно (исключая биты кадров, но включая байты FCS).
txHCPkt256to511Octets	Счетчик переданных 256 – 511-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 256 до 511 байт включительно (исключая биты кадров, но включая байты FCS).
txHCPkt512to1023Octets	Счетчик переданных 512 – 1023-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка

	Len/Type), от 512 до 1023 байт включительно (исключая биты кадров, но включая байты FCS).
txHCPkt1024to1518Octets	Счетчик переданных 1024 – 1518-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 1024 до 1518 байт включительно (исключая биты кадров, но включая байты FCS).
txHCPkt1519to1522Octets	Счетчик переданных допустимых 1519 – 1522-байтовых кадров VLAN. Возрастает с каждым допустимым кадром VLAN (исключая FCS, Symbol, ошибку TX), от 1519 до 1522 байт включительно (исключая биты кадров, но включая байты FCS).
txHCPkt1519to2047Octets	Счетчик переданных 1519 – 2047-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 1519 до 2047 байт включительно (исключая биты кадров, но включая байты FCS).
txHCPkt2048to4095Octets	Счетчик переданных 2048 – 4095-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 2048 до 4095 байт включительно (исключая биты кадров, но включая байты FCS).
txHCPkt4096to9216Octets	Счетчик переданных 4096 – 9216-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 4096 до 9216 байт включительно (исключая биты кадров, но включая байты FCS).
txHCPkt9217to16383Octets	Счетчик переданных 9217 – 16383-байтовых кадров. Возрастает с каждым допустимым и поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 9217 до 16383 байт включительно (исключая биты кадров, но включая байты FCS).
rxCRCAAlignErrors	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 имеющих либо поврежденный FCS с целым числом октетов (ошибка FCS), либо поврежденный FCS с не целым числом октетов (Ошибка выравнивания).
rxUndersizedPkts	Счетчик принятых кадров неполного размера. Возрастает с каждым принятым пакетом меньше 64 байт в длину (исключая биты кадров, но включая октеты FCS), но в остальном сформированным верно (содержащим допустимый FCS).
rxFragmentPkts	Счетчик принятых фрагментов. Возрастает с каждым принятым пакетом меньше 64 байт в длину (исключая биты кадров, но включая октеты FCS), но имеющих либо поврежденный FCS с целым числом октетов (ошибка FCS), либо поврежденный FCS с не целым числом октетов (Ошибка выравнивания).
rxSymbolErrors	Счетчик принятых кадров с ошибкой кода. Возрастает с каждым принятым кадром, содержащим недопустимый

	символ данных, но допустимый носитель.
txCollisions	Счетчик общего числа коллизий при передаче. Возрастает с общим числом коллизий, возникших во время передачи.
ifInErrors	Счетчик принятых пакетов с ошибкой. Возрастает при приеме пакетов, содержащих ошибки, не допускающие их дальнейшую передачу протоколу на уровень выше. Счетчик является суммой dot3StatsAlignmentErrors, dot3StatsFCSErrors, dot3StatsFrameTooLongs и dot3StatsInternalReceiveError.
ifOutErrors	Счетчик пакетов, переданных с ошибкой. Возрастает при попытке передачи пакетов, содержащих ошибки, не допускающих их дальнейшую передачу. Счетчик является суммой dot3StatsSQETestErrors, dot3StatsLateCollisions, dot3StatsExcessiveCollisions, dot3StatsInternalMacTransmitErrors и dot3StatsCarrierSenseErrors.
ifInDiscards	Счетчик отброшенных принятых пакетов. Возрастает при приеме пакетов, которые в дальнейшем отбрасываются по какой-либо причине. Например, MTU drop, Buffer Full Drop, ACL Drop, Multicast Drop, VLAN Ingress Drop, Invalid IPv6, STP Drop, Storm and FDB Discard и т.д.
ifOutDiscards	Счетчик отброшенных переданных пакетов. Возрастает при передаче пакетов, отброшенных в дальнейшем по какой-либо причине. Например, excessive transit delay discards, HOL drop, STP drop, MTU drop, VLAN drop, и т.д.
txDelayExceededDiscards	Счетчик просроченных переданных пакетов. Возрастает при передаче пакетов, которые были отброшены из-за превышения времени передачи.
txCRC	Счетчик переданных пакетов с ошибкой FCS. Возрастает с каждым переданным пакетом, не прошедшим проверку FCS.
dot3StatsSingleColFrames	Счетчик переданных кадров с одиночной коллизией. Доступен только для режима 10/100. Возрастает с каждым переданным кадром, испытавшим одну коллизию по время передачи.
dot3StatsMultiColFrames	Счетчик переданных кадров многочисленных коллизий. Доступен только в режиме 10/100. Возрастает с каждым успешно переданным кадром, испытавшим больше одной коллизии по время передачи.
dot3StatsDeferredTransmissions	Счетчик одиночных отложенных при передаче кадров. Доступен только в режиме 10/100. Возрастает с каждым переданным кадром, который был отложен при первой попытке передачи и в дальнейшем не подвергся коллизии во время последующей передачи.
dot3StatsLateCollisions	Счетчик кадров поздней коллизии. Доступен только в режиме 10/100. Возрастает с каждым переданным кадром с поздней коллизией во время попытки передачи.
dot3StatsExcessiveCollisions	Счетчик переданных кадров с избытком коллизий. Доступен только в режиме 10/100. Возрастает с каждым кадром, передача которого не состоялась из-за избытка

	коллизий.
dot3StatsInternalMacTransmitErrors	Счетчик переданных кадров с внутренней ошибкой MAC. Возрастает с каждым кадром, передача которого не состоялась из-за ошибки передачи внутреннего подуровня MAC. Кадр учитывается, только если он не был учтен никаким из следующих счетчиков: dot3StatsLateCollisions, dot3StatsExcessiveCollisions и dot3StatsCarrierSenseErrors.
dot3StatsFrameTooLongs	Счетчик принятых кадров слишком большой длины. Возрастает с каждым принятым кадром, превышающим размер max-rcv-frame-size.

41-6 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 loorback или другой интерфейс.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Если интерфейс не указан, отображаться будут данные для всех интерфейсов.

Пример

В данном примере показано, как включить отображение информации об интерфейсе VLAN для интерфейса VLAN 1.

```
Switch#show interfaces vlan 1

vlan 1 is enabled, Link status is up
  Interface type: VLAN
  Interface description:
  MAC address: F0-7D-68-36-30-B0

Switch#
```

В данном примере показано, как включить отображение информации об интерфейсе loopback для интерфейса loopback 1.

```
Switch# show interfaces loopback1

loopback1 is enabled, link status is up
Interface type: Loopback
Interface description: Loopback 1 for MIS

Switch#
```

В данном примере показано, как включить отображение информации об интерфейсе NULL для интерфейса null0.

```
Switch# show interfaces null0

Null0 is enabled, link status is up
Interface type: Null
Interface description: Null0 for MIS

Switch#
```

В данном примере показано, как включить отображение информации об интерфейсе для Ethernet 1/0/1.

```

Switch#show interfaces ethernet 1/0/1

Eth1/0/1 is enabled link status is up
  Interface type: 1000BASE-T
  Interface description:
  MAC Address: F0-7D-68-36-31-B0
  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, 100Mb/s
  Maximum transmit unit: 1536 bytes
  RX rate: 464 bits/sec, TX rate: 0 bits/sec
  RX bytes: 40795, TX bytes: 29789
  RX rate: 0 packets/sec, TX rate: 0 packets/sec
  RX packets: 559, TX packets: 61
  RX multicast: 43, RX broadcast: 0
  RX CRC error: 0, RX undersize: 0
  RX fragment: 0, RX dropped Pkts: 100
  RX MTU exceeded: 0
  TX CRC error: 0, TX excessive deferral: 0
  TX single collision: 0, TX excessive collision: 0
  TX late collision: 0, TX collision: 0

Switch#

```

В данном примере показано, как включить отображение информации об интерфейсе для порта управления (management port 0).

```

Switch#show interfaces mgmt 0

mgmt_ipif 0 is enabled, Link status is up
  Interface type: Management port

Switch#

```

41-7 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.
errors	(Опционально) Укажите для отображения счетчика ошибок.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения общих счетчиков, счетчиков ошибок или архивной информации для указанного или всех интерфейсов.

Пример

В данном примере показано, как включить отображение счетчиков порта RX коммутатора для портов 1 и 2.

```
Switch#show interfaces ethernet 1/0/1-2 counters

Port          InOctets /      InMcastPkts /
              InUcastPkts      InBcastPkts
-----
eth1/0/1      42651           43
              71             474
eth1/0/2      0               0
              0               0

Port          OutOctets /      OutMcastPkts /
              OutUcastPkts      OutBcastPkts
-----
eth1/0/1      29789           0
              61             0
eth1/0/2      0               0
              0               0

Total Entries:2

Switch#
```

В данном примере показано, как включить отображение счетчиков для ошибок на портах коммутатора.

```
Switch#show interfaces ethernet 1/0/1,1/0/3 counters errors

Port          CrcAlign-Err /      Undersize /
              Rcv-Err /          InDiscard /
              Xmit-Err          OutDiscard
-----
eth1/0/1      0                    0
              0                    100
              0                    0
eth1/0/3      0                    0
              0                    0
              0                    0

Port          Single-Col /      Excess-Col /
              Multi-Co /      Runts /
              Late-Col    Symbol-Err
-----
eth1/0/1      0                    0
              0                    0
              0                    0
eth1/0/3      0                    0
              0                    0
              0                    0

Port          DeferredTx      IntMacTx
-----
eth1/0/1      0                    0
eth1/0/3      0                    0

Total Entries:2

Switch#
```

Отображаемые параметры

Rcv-Err	Обратитесь к «ifInErrors» в разделе «Отображаемые параметры» команды show counters .
UnderSize	Обратитесь к «rxUndersizedPkts» в разделе «Отображаемые параметры» команды show counters .
Xmit-Err	Обратитесь к «ifOutErrors» в разделе «Отображаемые параметры» команды show counters .
OutDiscard	Обратитесь к «ifOutDiscards» в разделе «Отображаемые параметры» команды show counters .
Single-Col	Обратитесь к «dot3StatsSingleColFrames» в разделе «Отображаемые параметры» команды show counters .
Multi-Col	Обратитесь к «dot3StatsMultiColFrames» в разделе «Отображаемые параметры» команды show counters .
Late-Col	Обратитесь к «dot3StatsLateCollisions» в разделе «Отображаемые параметры» команды show counters .

Excess-Col	Обратитесь к «dot3StatsExcessiveCollisions» в разделе «Отображаемые параметры» команды show counters .
Symbol-Err	Обратитесь к «rxSymbolErrors» в разделе «Отображаемые параметры» команды show counters .
DeferredTx	Обратитесь к «txDelayExceededDiscards» в разделе «Отображаемые параметры» команды show counters .
IntMacTx	Обратитесь к «dot3StatsInternalMacTransmitErrors» в разделе «Отображаемые параметры» команды show counters .

41-8 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

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для просмотра состояния подключения портов коммутатора.

Пример

В данном примере показано, как включить отображение состояния подключения портов коммутатора.

```
Switch#show interfaces status
```

Port	Status	VLAN	Duplex	Speed	Type
eth1/0/1	connected	1	a-full	a-100	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	not-connected	1	auto	auto	1000BASE-T
eth1/0/9	not-connected	1	auto	auto	1000BASE-T
eth1/0/10	not-connected	1	auto	auto	1000BASE-T
eth1/0/11	not-connected	1	auto	auto	1000BASE-T
eth1/0/12	not-connected	1	auto	auto	1000BASE-T
eth1/0/13	not-connected	1	auto	auto	1000BASE-T
eth1/0/14	not-connected	1	auto	auto	1000BASE-T
eth1/0/15	not-connected	1	auto	auto	1000BASE-T
eth1/0/16	not-connected	1	auto	auto	1000BASE-T
eth1/0/17	not-connected	1	auto	auto	1000BASE-T
eth1/0/18	not-connected	1	auto	auto	1000BASE-T
eth1/0/19	not-connected	1	auto	auto	1000BASE-T
eth1/0/20	not-connected	1	auto	auto	1000BASE-T
eth1/0/21(c)	not-connected	1	auto	auto	1000BASE-T
eth1/0/21(f)	not-connected	1	auto	auto	1000BASE-T
eth1/0/22(c)	not-connected	1	auto	auto	1000BASE-T
eth1/0/22(f)	not-connected	1	auto	auto	1000BASE-T
eth1/0/23(c)	not-connected	1	auto	auto	1000BASE-T
eth1/0/23(f)	not-connected	1	auto	auto	1000BASE-T
eth1/0/24(c)	not-connected	1	auto	auto	1000BASE-T
eth1/0/24(f)	not-connected	1	auto	auto	1000BASE-T
eth1/0/25	not-connected	1	auto	auto	10GBASE-R
eth1/0/26	not-connected	1	auto	auto	10GBASE-R
eth1/0/27	not-connected	1	auto	auto	10GBASE-R
eth1/0/28	not-connected	1	auto	auto	10GBASE-R

Total Entries: 28

```
Switch#
```

41-9 show interfaces utilization

Данная команда используется для просмотра информации о загрузке портов коммутатора.

show interfaces [INTERFACE-ID [, | -]] utilization

Параметры

INTERFACE-ID

(Опционально) Укажите interface ID. Если параметр не указан, отображаться будет информация о загрузке всех

	физических портов коммутатора.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
utilization	(Опционально) Укажите для отображения информации о загрузке.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Команда позволяет пользователю просмотреть информацию о загрузке всех или указанных интерфейсов, так и архивную информацию об использовании CPU и памяти коммутатора.

Статистическая информация о скорости port-channel представляет собой сумму всех скоростей физических интерфейсов портов для данного port-channel. Например, интерфейсы физических портов с Ethernet 1/0/1 по Ethernet 1/0/4 принадлежат к одному и тому же port-channel, скорость приема (RX) данных (пакеты в секунду) для каждого порта 100, 200, 200, 100. Таким образом, скорость ошибок CRC данного port-channel будет 600 пакетов в секунду.

Пример

В данном примере показано отображение информации о загрузке портов коммутатора.

```
Switch#show interfaces utilization

Port          TX packets/sec  RX packets/sec  Utilization
-----
eth1/0/1      0                0                0
eth1/0/2      0                0                0
eth1/0/3      0                0                0
eth1/0/4      0                0                0
eth1/0/5      0                0                0
eth1/0/6      0                0                0
eth1/0/7      0                0                0
eth1/0/8      0                0                0
eth1/0/9      0                0                0
eth1/0/10     0                0                0
eth1/0/11     0                0                0
eth1/0/12     0                0                0
eth1/0/13     0                0                0
eth1/0/14     0                0                0
eth1/0/15     0                0                0
eth1/0/16     0                0                0
eth1/0/17     0                0                0
eth1/0/18     0                0                0
eth1/0/19     0                0                0
eth1/0/20     0                0                0
eth1/0/21     0                0                0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

41- 10 show interfaces gbic

Данная команда используется для просмотра информации о состоянии GBIC.

show interfaces [INTERFACE-ID [, | -]] gbic

Параметры

<i>INTERFACE-ID</i>	(Опционально) Укажите interface ID. Если параметр не указан, отображаться будет информация о состоянии GBIC для всех интерфейсов GBIC.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
gbic	Отображение информации о состоянии GBIC.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для просмотра информации о состоянии GBIC.

Пример

В данном примере показано отображение информации о состоянии GBIC.

```
Switch#show interfaces ethernet 1/0/1 gbic
eth1/0/1
  Interface Type: 1000BASE-T
Switch#
```

41-11 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.
auto-negotiation	Укажите для отображения подробной информации об автосогласовании.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для просмотра детальной информации об автосогласовании.

Пример

В данном примере показано отображение информации об автосогласовании.

```
Switch#show interfaces ethernet 1/0/1 auto-negotiation

eth1/0/1
  Auto Negotiation: Enabled

  Speed auto downgrade: Disabled
  Remote Signaling: Not detected
  Configure Status: Complete
  Capability Bits: 10M_Full, 100M_Full, 1000M_Full
  Capability Advertised Bits: 10M_Full, 100M_Full, 1000M_Full
  Capability Received Bits: 10M_Full, 100M_Full
  RemoteFaultAdvertised: Disabled
  RemoteFaultReceived: NoError

Switch#
```

41-12 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.
description	Укажите для отображения описания и состояния интерфейсов.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для 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
```

41-13 shutdown

Данная команда используется для отключения интерфейса. При использовании формы **no** включит включит интерфейс.

shutdown
no shutdown

Параметры

Нет

По умолчанию

По умолчанию выбрана опция **no shutdown**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться для отключения интерфейсов физического порта, loopback, VLAN, Tunnel и интерфейсов управления. Команда также может использоваться для портов port- channel.

Команда отключает порт. В отключенном состоянии порт не будет принимать или передавать пакеты. Используйте команду **no shutdown**, чтобы снова включить порт. Если порт отключен, подключение к сети также будет невозможно, и соединения не будет.

Пример

В данном примере показано, как отключить порт 1/0/1 с помощью данной команды.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#shutdown
Switch(config-if)#
```


42. Команды Internet Group Management Protocol(IGMP) Snooping

42-1 clear ip igmp snooping statistics

Данная команда используется для удаления статистики IGMP Snooping.

```
clear ip igmp snooping statistics {all | vlan VLAN-ID | interface INTERFACE-ID}
```

Параметры

all	Укажите, чтобы удалить статистику IP IGMP Snooping для всех VLAN и портов.
vlan VLAN-ID	Укажите VLAN, для которой необходимо удалить статистику IP IGMP Snooping.
interface INTERFACE-ID	Укажите порт, для которого необходимо удалить статистику IP IGMP Snooping.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы удалить статистику IGMP Snooping.

Пример

В данном примере показано, как удалить всю статистику IGMP Snooping.

```
Switch# clear ip igmp snooping statistics all
Switch#
```

42-2 ip igmp snooping

Данная команда используется для включения функции IGMP Snooping на коммутаторе. Используйте форму **no**, чтобы отключить данную функцию.

```
ip igmp snooping
no ip igmp snooping
```

Параметры

Нет

По умолчанию

Функция IGMP Snooping отключена на всех интерфейсах VLAN.
Функция IGMP Snooping отключена глобально.

Режим ввода команды

Interface Configuration Mode
Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

В режиме Interface Configuration Mode команда может быть использована только для настройки интерфейса VLAN. Для того, чтобы предоставить VLAN доступ к IGMP Snooping, необходимо включить данную функцию глобально и для интерфейса. Настройки IGMP Snooping и MLD Snooping являются независимыми и могут быть применены для VLAN одновременно.

Пример

В данном примере показано, как отключить функцию IGMP Snooping на всех VLAN.

```
Switch# configure terminal
Switch(config)# no ip igmp snooping
Switch(config)#
```

В данном примере показано, как включить функцию IGMP Snooping на всех VLAN.

```
Switch# configure terminal
Switch(config)# ip igmp snooping
Switch(config)#
```

В данном примере показано, как отключить функцию IGMP Snooping на VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# no ip igmp snooping
Switch(config-vlan)#
```

42-3 ip igmp snooping access-group

Данная команда используется для того, чтобы ограничить подключение клиентов подсети, разрешив им подключаться только к многоадресным группам, внесенным в стандартный список доступа IP. Используйте форму **no**, чтобы отключить данную функцию.

```
ip igmp snooping access-group ACCESS-LIST-NAME [vlan VLAN-ID]
no ip igmp snooping access-group [vlan VLAN-ID]
```

Параметры

<i>ACCESS-LIST-NAME</i>	Укажите стандартный список доступа IP. Чтобы разрешить пользователям подключиться к группе (*, G), укажите «any» в поле адреса источника (source) и G в поле адреса назначения (destination) записи списка доступа.
vlan <i>VLAN-ID</i>	(Опционально) Укажите VLAN на trunk-порту, чтобы включить фильтрацию пакетов, прибывающих на данную VLAN.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду **ip igmp snooping access-group**, чтобы ограничить подключение получателей многоадресного трафика к указанной группе. Часть адреса назначения списка доступа отображает адрес многоадресной группы, к которой разрешено / запрещено подключаться клиенту.

Данная команда применима для настройки интерфейсов физического порта и port-channel.

Пример

В данном примере показано, как выбрать группу 226.1.1.1 в качестве единственной разрешенной обслуживаемой группы IGMP Snooping для интерфейса ethernet 1/0/1. Сначала создайте список доступа IP-адресов «igmp_filter», разрешающий только пакеты, предназначенные для группы 226.1.1.1. Затем ассоциируйте данную группу доступа с интерфейсом ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# ip access-list igmp_filter
Switch(config-ip-acl)# permit any host 226.1.1.1
Switch(config-ip-acl)# end
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ip igmp snooping access-group igmp_filter
Switch(config-if)#
```

42-4 ip igmp snooping accounting

Данная команда используется для включения IGMP Accounting при подключении получателя к IGMP-группе. Используйте форму **no**, чтобы отключить данную функцию.

ip igmp snooping accounting
no ip igmp snooping accounting

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и port-channel. Используйте данную команду, чтобы включить/отключить IGMP Accounting при подключении получателя к IGMP-группе. Если данная функция включена, при подключении получателя к группе на RADIUS будет выслано сообщение IGMP Accounting.

Пример

В данном примере показано, как включить IGMP Accounting на интерфейсе ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#ip igmp snooping accounting
Switch(config-if)#
```

42-5 ip igmp snooping authentication

Данная команда используется для того, чтобы включить функцию аутентификации для сообщений IGMP Join. Используйте форму **no**, чтобы отключить данную функцию.

ip igmp snooping authentication
no ip igmp snooping authentication

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и port-channel. Используйте данную команду, чтобы включить/отключить функцию аутентификации для сообщений IGMP Join. Если данная функция включена, при попытке подключения клиента к группе сначала будет проведена аутентификация.

Пример

В данном примере показано, как включить функцию аутентификации на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#ip igmp snooping accounting
Switch(config-if)#
```

42-6 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

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Используйте команду **ip igmp snooping fast-leave**, чтобы удалить членство IGMP на порту после получения сообщения Leave, не применяя механизм обработки сообщений Group-Specific Query (с указанием группы) или Group-Source-Specific Query (с указанием источника группы).

Пример

В данном примере показано, как включить функцию IGMP Snooping Fast Leave на VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping fast-leave
Switch(config-vlan)#
```

42-7 ip igmp snooping ignore-topology-change-notification

Данная команда используется для игнорирования изменений STP и отказа от отправки на интерфейс STP-запроса. Используйте форму **no**, чтобы отключить игнорирование изменений STP и отправлять STP-запросы на интерфейс.

```
ip igmp snooping ignore-topology-change-notification
no ip igmp snooping ignore-topology-change-notification
```

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Коммутатор с включенной функцией IGMP Snooping получает информацию об изменениях топологии Link Layer, вызванных Spanning Tree. Если порт включен/отключен при помощи Spanning Tree, на все активные порты, кроме router-портов, будет отправлено сообщение General Query, чтобы сократить интервал сетевой конвергенции. Используйте данную команду, чтобы игнорировать случаи изменения топологии.

Пример

В данном примере показано, как включить игнорирование изменений топологии на VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping ignore-topology-change-notification
Switch(config-vlan)#
```

42-8 ip igmp snooping last-member-query-interval

Данная команда используется для настройки интервала, в течение которого IGMP Snooping Querier отправляет сообщения Group-Specific Query (с указанием группы) или Group-Source-Specific Query (с указанием источника группы) / Channel-Source-Specific Query (с указанием источника канала). Используйте форму **no**, чтобы вернуться 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

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Получив сообщение IGMP Leave, IGMP Snooping Querier будет считать, что на интерфейсе нет локальных участников, если по истечении времени ожидания не будет получено ни одного ответа. Пользователи могут уменьшить данный интервал, чтобы сократить время, которое уходит у коммутатора на обнаружение потери последнего участника группы.

Пример

В данном примере показано, как настроить значение last member query interval. Указанное значение – 3 секунды.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping last-member-query-interval 3
Switch(config-vlan)#
```

42-9 ip igmp snooping limit

Данная команда используется для установки ограничения по количеству записей кэша IGMP, которые можно создать. Используйте форму **no**, чтобы удалить ограничение.

```

ip igmp snooping limit NUMBER [exceed-action {drop | replace}] [except ACCESS-LIST-NAME][vlan
VLAN-ID]
no ip igmp snooping limit [vlan VLAN-ID]

```

Параметры

<i>NUMBER</i>	Укажите максимальное количество записей кэша IGMP, которое можно создать. Доступный диапазон значений: от 1 до 8192.
exceed-action	(Опционально) Укажите действие для изученных групп, если лимит превышен.
drop	(Опционально) Укажите, чтобы отбросить новую группу.
replace	(Опционально) Укажите, чтобы заменить старую группу новой.
except <i>ACCESS-LIST-NAME</i>	(Опционально) Укажите стандартный список доступа IP. Для группы (*,G) или канала (S,G), внесенных в список доступа, ограничения не будут установлены. Чтобы не устанавливать ограничения для канала (S,G), укажите S в поле адреса ис- точника и G в поле адреса назначения записи списка доступа. Чтобы не устанавливать ограничения для группы (*,G), укажите “any” в поле адреса источника и G в поле адреса назначения записи списка доступа.
vlan <i>VLAN-ID</i>	(Опционально) Укажите VLAN уровня 2, чтобы включить фильтрацию пакетов, прибывающих на данную VLAN.

По умолчанию

По умолчанию ограничения отсутствуют.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применима для настройки интерфейсов физического порта и port-channel. Параметр **except** позволяет указать стандартный список доступа групп или каналов, для которых не будут установлены ограничения.

Пример

В данном примере показано, как установить ограничение по количеству групп IGMP Snooping с лимитом настройки от ACL, к которому может подключиться интерфейс ethernet 1/0/4 с VLAN ID 1000.


```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/4
Switch(config-if)# ip igmp snooping limit 80 except igmp_filter vlan 1000
Switch(config-if)#
```

В данном примере показано, как установить ограничение по количеству групп IGMP Snooping по умолчанию, к которому может подключиться интерфейс port-channel 4 с VLAN ID 1000.

```
Switch# configure terminal
Switch(config)# interface port-channel 4
Switch(config-if)# no ip igmp snooping limit vlan 1000
Switch(config-if)#
```

42-10 ip igmp snooping mrouter

Данная команда используется для настройки указанного интерфейса/интерфейсов в качестве multicast router-портов, а также для указания интерфейса/интерфейсов, которые не могут быть multicast router-портами. Используйте форму **no**, чтобы удалить интерфейс/интерфейсы из списка router-портов или списка запрещенных router-портов.

ip igmp snooping mrouter {interface *INTERFACE-ID* [, | -] | forbidden interface *INTERFACE-ID* [, | -]}

no ip igmp snooping mrouter {interface *INTERFACE-ID* [, | -] | forbidden interface *INTERFACE-ID* [, | -]}

Параметры

interface	Укажите статический multicast router-порт.
forbidden interface	Укажите порт, который не может быть multicast router-портом.
<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

По умолчанию multicast router-порты IGMP Snooping отсутствуют.

По умолчанию включено автоматическое изучение.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. multicast router-портом можно назначить физический порт или port-channel. Указанный multicast router-порт должен являться портом-участником сконфигурированной VLAN. Multicast router-порт может быть изучен динамически или сконфигурирован статически. При помощи динамического изучения устройство IGMP Snooping будет изучать пакеты IGMP, PIM или DVMRP, чтобы идентифицировать multicast router-порт. Если автоматическое изучение отключено, multicast router-порт может быть только сконфигурирован статически.

Пример

В данном примере показано, как добавить статический multicast router-порт IGMP Snooping для VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping mrouter interface ethernet 1/0/4
Switch(config-vlan)#
```

42-11 ip igmp snooping proxy-reporting

Данная команда используется для включения функции Proxy Reporting. Используйте форму **no**, чтобы отключить данную функцию.

```
ip igmp snooping proxy-reporting [source IP-ADDRESS]
no ip igmp snooping proxy-reporting
```

Параметры

source IP-ADDRESS	(Опционально) Укажите IP-адрес источника (source) Proxy Reporting. Значение по умолчанию составляет 0.
--------------------------	--

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Если функция Proxy Reporting включена, перед отправкой на router-порт полученные пакеты IGMP Report или IGMP Leave для указанного канала (S, G) будут объединены в один отчет. В качестве IP-адреса источника отчета будет использован IP-адрес источника Proxy Reporting. Если IP-адрес источника Proxy Reporting не настроен, будет использован нулевой IP-адрес. MAC-адрес интерфейса будет использован в качестве MAC-адреса источника отчета. Если на VLAN нет настроенных IP-адресов, будет использован системный MAC-адрес.

Пример

В данном примере показано, как включить IGMP Snooping Proxy Reporting на VLAN 1 и настроить IP-адрес источника сообщения Proxy Reporting. Настроенный IP-адрес – 1.2.2.2.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-if)# ip igmp snooping proxy-reporting source 1.2.2.2
Switch(config-if)#
```

42-12 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

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Чтобы запустить Querier, интерфейсу необходимо присвоить IP-адрес. Если у VLAN отсутствует IP-адрес, система вышет сообщение Warning. Если Querier включен, но IP-адрес удален, работа Querier будет остановлена. Если система может выполнить роль Querier, устройство будет ожидать пакеты IGMP Query, отправленные другими устройствами. При получении сообщения IGMP Query устройство с более низким значением IP-адреса становится Querier. Если на интерфейсе также включен IGMP-протокол, IGMP Snooping Querier будет автоматически отключен.

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)#
```

42-13 ip igmp snooping query-interval

Данная команда используется для настройки интервала между сообщениями IGMP General Query. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip igmp snooping query-interval SECONDS  
no ip igmp snooping query-interval
```

Параметры

<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

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Query Interval – это интервал между сообщениями General Query, отправленными Querier. Администратор может настраивать количество IGMP-сообщений, изменяя значение данного интервала: чем больше значение интервала, тем реже будут отправляться сообщения IGMP Query.

Пример

В данном примере показано, как настроить интервал IGMP Snooping Query на VLAN 1000. Указанное значение – 300 секунд.

```
Switch# configure terminal  
Switch(config)# vlan 1000  
Switch(config-vlan)# ip igmp snooping query-interval 300  
Switch(config-vlan)#
```

42-14 ip igmp snooping query-max-response-time

Данная команда используется для настройки максимального значения времени ожидания, анонсированного в сообщениях IGMP Snooping Query. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip igmp snooping query-max-response-time SECONDS  
no ip igmp snooping query-max-response-time
```

Параметры

SECONDS

Укажите максимальное значение времени ожидания, анонсированное в сообщениях IGMP Snooping Query. Доступный диапазон значений: от 1 до 25 секунд.

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Используйте данную команду, чтобы настроить период времени, в течение которого участник группы может ответить на сообщение IGMP Query, прежде чем его участие будет удалено посредством IGMP Snooping.

Пример

В данном примере показано, как настроить максимальное значение времени ожидания на 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)#
```

42-15 ip igmp snooping query-version

Данная команда используется для настройки версии пакетов General Query, отправляемых IGMP Snooping Querier. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip igmp snooping query-version NUMBER
no ip igmp snooping query-version
```

Параметры**NUMBER**

Укажите версию пакета IGMP General Query, отправленного IGMP Snooping Querier. Доступный диапазон значений: от 1 до 3.

По умолчанию

Значение по умолчанию – 3.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Настройки версии пакета Query повлияют на выбор Querier. Если выбрана версия 1, IGMP Snooping действует в качестве Querier и не инициирует выбор нового Querier вне зависимости от того, какой пакет IGMP Query получен. Если выбрана версия 2 или 3, IGMP Snooping инициирует выбор нового Querier при получении пакета IGMPv2 или IGMPv3, и не инициирует выбор нового Querier при получении пакета IGMPv1.

Пример

В данном примере показано, как настроить версию пакета Query на VLAN 1000. Указанная версия – 2.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping query-version 2
Switch(config-vlan)#
```

42-16 ip igmp snooping rate-limit

Данная команда используется для ограничения скорости передачи входящих управляющих IGMP- пакетов. Используйте форму **no**, чтобы отключить ограничения по скорости.

```
ip igmp snooping rate-limit NUMBER
no ip igmp snooping rate-limit
```

Параметры

<i>NUMBER</i>	Укажите пропускную способность (количество пакетов в секунду) для управляющих IGMP-пакетов, обработка которых возможна на определенном интерфейсе.
---------------	--

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться для настройки интерфейса VLAN, физического порта и port-channel. Используйте данную команду, чтобы настроить скорость передачи управляющих IGMP- пакетов, которые могут быть обработаны IGMP Snooping.

Пример

В данном примере показано, как ограничить скорость передачи пакетов на интерфейсе VLAN 1000. Указанное ограничение – 30 пакетов в секунду.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping rate-limit 30
Switch(config-vlan)#
```

42- 17 ip igmp snooping report-suppression

Данная команда используется для включения функции report suppression. Используйте форму **no**, чтобы отключить данную функцию.

```
ip igmp snooping report-suppression
no ip igmp snooping report-suppression
```

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Функция report suppression работает только для трафика IGMPv1 и IGMPv2. Если функция report suppression включена, коммутатор блокирует дублированные отчеты, отправленные узлами. Сообщения IGMP Report или IGMP Leave одной группы будут блокироваться до тех пор, пока не истечет установленное время. Для одной группы будет передано только одно сообщение IGMP Report или IGMP Leave, остальные сообщения будут заблокированы.

Пример

В данном примере показано, как включить функцию report suppression на VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping report-suppression
Switch(config-vlan)#
```

42-18 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

<i>VALUE</i>	Укажите значение robustness variable в диапазоне от 1 до 7.
--------------	---

По умолчанию

Значение по умолчанию – 2.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Robustness variable обеспечивает точную настройку в соответствии с ожидаемой потерей пакетов на интерфейсе. Значение robustness variable используется для расчета следующих интервалов IGMP-сообщений:

- **Group member interval** – промежуток времени, по истечении которого маршрутизатор считает, что в группе больше нет активных участников. Данный интервал рассчитывается следующим образом: (robustness variable x query interval) + (1 x query response interval).
- **Other querier present interval** – промежуток времени, по истечении которого многоадресный маршрутизатор считает, что маршрутизатор, являющийся Querier, больше не доступен. Данный интервал рассчитывается следующим образом: (robustness variable x query interval) + (0.5 x query response interval).
- **Last member query count** – количество запросов Group-Specific Queries (с указанием группы), отправленных маршрутизатором до того, как он предполагает, что в группе нет локальных участников. Robustness variable является значением по умолчанию данного счетчика.

Пользователи могут увеличить данное значение, если для сети требуются более свободные условия.

Пример

В данном примере показано, как настроить robustness variable на интерфейсе VLAN 1000. Указанное значение – 3.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping robustness-variable 3
Switch(config-vlan)#
```

42-19 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.
interface <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

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Используйте данную команду на интерфейсе VLAN, чтобы добавить запись статической группы и/или источник multicast потока.

Используйте команду **ip igmp snooping static-group**, чтобы создать статическую группу IGMP Snooping, если подключенный узел не поддерживает IGMP-протокол.

Пример

В данном примере показано, как добавить запись статической группы 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)#
```

42-20 ip igmp snooping suppression-time

Данная команда используется для настройки интервала, в течение которого будут блокированы дублированные сообщения IGMP Report или IGMP Leave. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip igmp snooping suppression-time SECONDS
no ip igmp snooping suppression-time
```

Параметры

<i>SECONDS</i>	Укажите интервал блокирования дублированных сообщений IGMP Report. Доступный диапазон значений: от 1 до 300.
----------------	--

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Функция report suppression блокирует дублированные пакеты IGMP Report или IGMP Leave, полученные в течение указанного интервала. Чем меньше значение интервала suppression, тем чаще будут отправляться дублированные IGMP-пакеты.

Пример

В данном примере показано, как настроить интервал suppression на VLAN 1000. Указанное значение – 125.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping suppression-time 125
Switch(config-vlan)#
```

42-21 ip igmp snooping minimum-version

Данная команда используется для настройки минимальной версии IGMP-узлов, разрешенной на интерфейсе. Используйте форму **no**, чтобы удалить ограничение.

```
ip igmp snooping minimum-version {2 | 3}
no ip igmp snooping minimum-version
```

Параметры

2	Укажите, чтобы отфильтровать сообщения IGMPv1.
3	Укажите, чтобы отфильтровать сообщения IGMPv1 и IGMPv2.

По умолчанию

По умолчанию ограничения минимальной версии отсутствуют.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда может применяться только для настройки интерфейса VLAN. Настройки применимы только для фильтрации сообщений IGMP Membership Report.

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)#
```

42-22 show ip igmp snooping

Данная команда используется для отображения информации об IGMP Snooping на коммутаторе.

show ip igmp snooping [vlan VLAN-ID]

Параметры

vlan VLAN-ID	(Опционально) Укажите VLAN, которую необходимо отобразить.
---------------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию об IGMP Snooping для всех VLAN, на которых включена данная функция.

Пример

В данном примере показано, как отобразить настройки IGMP Snooping.

```

Switch#show ip igmp snooping

IGMP snooping global state: Enabled

VLAN #1 configuration
  IGMP snooping state      : Enabled
  Minimum version          : v1
  Fast leave               : Disabled (host-based)
  Report suppression      : Disabled
  Suppression time        : 10 seconds
  Querier state            : Disabled
  Query version            : v3
  Query interval           : 125 seconds
  Max response time       : 10 seconds
  Robustness value        : 2
  Last member query interval : 1 seconds
  Proxy reporting         : Disabled (Source 0.0.0.0)
  Rate limit               : 0
  Ignore topology change  : Disabled

Total Entries: 1

Switch#

```

42-23 show ip igmp snooping aaa

Данная команда используется для отображения информации об аутентификации IGMP Snooping и конфигурации IGMP Accounting.

show ip igmp snooping aaa [interface *INTERFACE-ID* [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите интерфейс или список интерфейсов. Может быть использован физический интерфейс или port-channel.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию об аутентификации IGMP Snooping и конфигурации IGMP Accounting. Если не указаны дополнительные параметры, будет отображена информация для всех интерфейсов.

Пример

В данном примере показано, как отобразить информацию об аутентификации IGMP Snooping и конфигурации IGMP Accounting.

```
Switch#show ip igmp snooping aaa
Authentication enabled interface:
1/0/1-1/0/5
Accounting enabled interface:
1/0/1-1/0/5
Switch#
```

42-24 show ip igmp snooping groups

Данная команда используется для отображения информации о группе IGMP Snooping, изученной на коммутаторе.

show ip igmp snooping groups [vlan VLAN-ID [, | -] | [IP-ADDRESS] [detail]

Параметры

vlan VLAN-ID	(Опционально) Укажите интерфейс VLAN, который необходимо отобразить. Если VLAN не указаны, будет отображена информация о группе IGMP Snooping для всех VLAN с включенной функцией IGMP Snooping.
,	(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.
IP-ADDRESS	(Опционально) Укажите IP-адрес группы, которую необходимо отобразить. Если IP-адрес не указан, будет отображена информация обо всех группах IGMP.
detail	(Опционально) Укажите, чтобы отобразить подробную информацию о группе IGMP.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию о группе IGMP Snooping.

Пример

В данном примере показано, как отобразить информацию о группе IGMP Snooping.

```
Switch# show ip igmp snooping groups

Total Group Entries : 1
Total Source Entries: 2

vlan 1, 230.1.1.1
Learned on port: 1/0/3,1/0/5

Switch#
```

42-25 show ip igmp snooping filter

Данная команда используется для отображения информации о конфигурации IGMP Snooping Filter для всех интерфейсов или для указанного интерфейса.

show ip igmp snooping filter [interface *INTERFACE-ID* [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите физический интерфейс или port-channel. Если интерфейс не указан, будет отображена информация об IGMP Snooping Filter для всех интерфейсов.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию о группе доступа и ограничении IGMP Snooping.

Пример

В данном примере показано, как отобразить информацию об IGMP Snooping Filter, если интерфейс не указан.

```
Switch#show ip igmp snooping filter

eth1/0/1
  Rate limit: Not Configured
  Access group: Not Configured
  Groups/Channel Limit: Not Configured
  vlan 1:
    Access group: Not Configured
    Groups/Channel Limit: 100 (Exception List: AccessList, exceed-action: drop)

eth1/0/2
  Rate limit: 10pps
  Access group: Not Configured
  Groups/Channel Limit: Not Configured
  vlan 1:
    Access group: Not Configured
    Groups/Channel Limit: 100 (Exception List: ExtendACL, exceed-action: drop)

Switch#
```

В данном примере показано, как отобразить информацию об IGMP Snooping Filter для интерфейса Ethernet 1/0/2.


```
Switch#show ip igmp snooping filter interface ethernet 1/0/2

eth1/0/2
  Rate limit: 10pps
  Access group: Not Configured
  Groups/Channel Limit: Not Configured
  vlan 1:
    Access group: Not Configured
    Groups/Channel Limit: 100 (Exception List: ExtendACL, exceed-action: drop)

Switch#
```

42-26 show ip igmp snooping mrouter

Данная команда используется для отображения информации о многоадресном маршрутизаторе IGMP Snooping, который был автоматически изучен и настроен вручную.

show ip igmp snooping mrouter [vlan VLAN-ID [, | -]]

Параметры

vlan VLAN-ID	(Опционально) Укажите VLAN. Если VLAN не указана, будет отображена информация об IGMP Snooping на всех VLAN с включенной функцией IGMP Snooping.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить интерфейсы динамически изученного или настроенного вручную многоадресного маршрутизатора.

Пример

В данном примере показано, как отобразить информацию о многоадресном маршрутизаторе IGMP Snooping.

```
Switch#show ip igmp snooping mrouter

VLAN  Ports
-----
1     1/0/1-1/0/4 (static)

Total Entries: 1

Switch#
```

42-27 show ip igmp snooping statistics

Данная команда используется для отображения информации о статистике IGMP Snooping на коммутаторе.

show ip igmp snooping statistics {interface [INTERFACE-ID [, | -]] | vlan [VLAN-ID [, | -]]}

Параметры

interface	Укажите, чтобы отобразить счетчики статистики интерфейса.
<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.
vlan	Укажите, чтобы отобразить счетчики статистики VLAN.
<i>VLAN-ID</i>	(Опционально) Укажите VLAN ID, который необходимо отобразить.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию о статистике IGMP Snooping.

Пример

В данном примере показано, как отобразить информацию о статистике IGMP Snooping.

```
Switch#show ip igmp snooping statistics vlan 1

VLAN 1 Statistics:
  IGMPv1 Rx: Report 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#
```

42-28 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.
vlan <i>VLAN-ID</i>	(Опционально) Укажите VLAN ID, который необходимо отобразить.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить статически настроенные группы IGMP Snooping на коммутаторе. Если дополнительные параметры не выбраны, будет отображена вся информация.

Пример

В данном примере показано, как отобразить статически настроенные группы IGMP Snooping.

```
Switch#show ip igmp snooping static-group

VLAN ID  Group address  Interface
-----  -
1        230.1.1.1      1/0/1-1/0/2

Total Entries: 1

Switch#
```

43. Команды L3 Control Packet Filtering

43-1 cpu-filter l3-control-pkt

Данная команда используется для отбрасывания пакетов управления 3 уровня, отправленных на ЦПУ с указанных портов. Используйте форму **no**, чтобы остановить отбрасывание пакетов управления 3 уровня, отправленных на ЦПУ.

```
cpu-filter l3-control-pkt type [PACKET-TYPE]
no cpu-filter l3-control-pkt type [PACKET-TYPE]
```

Параметры

<i>PACKET-TYPE</i>	(Опционально) Укажите пакеты управления 3 уровня, которые необходимо сконфигурировать. Поддерживаются следующие типы пакетов управления 3 уровня: <ul style="list-style-type: none"> • dvmrp: Distance Vector Multicast Routing Protocol. • igmp-query: Internet Group Management Protocol Query. • ospf: Open Shortest Path First Protocol. • pim: Protocol Independent Multicast. • rip: Routing Information Protocol • vrrp: Virtual Router Redundancy Protocol.
--------------------	---

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы отбросить пакеты управления 3 уровня, отправленные на ЦПУ с указанных портов.

Пример

В данном примере показано, как отбросить пакеты DVMRP, отправленные на ЦПУ.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/2
Switch(config-if)#cpu-filter l3-control-pkt type dvmrp
Switch(config-if)#
```

43-2 show cpu-filter l3-control-pkt

Данная команда используется для отображения статуса фильтрации ЦПУ пакетов управления 3 уровня.

show cpu-filter l3-control-pkt [interface *INTERFACE-ID*]

Параметры

<i>INTERFACE-ID</i>	(Опционально) Укажите интерфейс (физический порт или port-channel). Если интерфейс не указан, будет отображена информация о фильтре IGMP Snooping на всех интерфейсах.
---------------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить статус фильтрации ЦПУ пакетов управления 3 уровня.

Пример

В данном примере показано, как отобразить статус фильтрации ЦПУ пакетов управления 3 уровня.

```
Switch#show cpu-filter l3-control-pkt

eth1/0/2
  Filter packet: DVMRP

Switch#
```

44. Команды IP Source Guard

44-1 ip verify source vlan dhcp-snooping

Данная команда используется для включения IP Source Guard на порту. При использовании формы **no** команда отключит IP Source Guard.

```
ip verify source vlan dhcp-snooping [ip-mac]
no ip verify source vlan dhcp-snooping [ip-mac]
```

Параметры

ip-mac	(Опционально) Укажите для проверки и IP, и MAC-адреса получаемых IP-пакетов.
---------------	--

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для настройки физического порта и port-channel. Используйте команду для включения IP Source Guard на необходимом порту.

При включении на порту IP Source Guard IP-пакеты, приходящие на порт, будут проверяться списком управления доступом (ACL). Порт списка управления доступом (порт ACL) – аппаратный механизм. Его записи могут быть настроены вручную либо получены с помощью таблицы привязки DHCP. Пакет, не прошедший проверку, будет отброшен.

Существует два типа проверки:

- Если не указан ip-mac, проверка основана только на IP-адресе источника и VLAN.
- Если указан ip-mac, проверка основана на MAC-адресе источника, VLAN и IP-адресе источника.

Пример

В данном примере показано, как включить IP Source Guard для Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config-if)#
```

44-2 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.
vlan <i>VLAN-ID</i>	Укажите VLAN, которой принадлежит проверенный узел.
<i>IP-ADDRESS</i>	Укажите IP-адрес для привязки IP-to-MAC.
interface <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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для создания статической привязки, используемой для проверки IP Source Guard. При использовании формы **no** команда удалит статическую привязку. Указанные параметры команды должны в точности совпадать с настроенными параметрами для удаления.

Если MAC-адрес и VLAN настраиваемой привязки уже есть, существующая привязка будет обновлена. Интерфейсом, указанным для команды, может быть физический порт или port-channel.

Пример

В данном примере показано, как настроить привязку IP Source Guard с IP-адресом 10.1.1.1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 Ethernet 1/0/10.

```
Switch# configure terminal
Switch(config)# ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface ethernet 1/0/10
Switch(config)#
```

В данном примере показано, как удалить привязку IP Source Guard с IP-адресом 10.1.1.1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 Ethernet 1/0/10.


```
Switch# configure terminal
Switch(config)# no ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface ethernet
1/0/10
Switch(config)#
```

44-3 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.
dhcp-snooping	(Опционально) Укажите для отображения привязки IP Source, изученной при помощи DHCP Snooping.
static	(Опционально) Укажите для отображения привязки IP Source Guard, настроенной вручную.
vlan <i>VLAN-ID</i>	(Опционально) Укажите для отображения привязки IP Source Guard на основе VLAN.
interface <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

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Записи привязки IP Source Guard либо настраиваются вручную, либо изучаются автоматически с помощью DHCP Snooping для защиты IP-трафика.

Пример

В данном примере показано, как настроить отображение привязки IP Source Guard без каких-либо параметров.

```
Switch#show ip source binding

MAC Address      IP Address      Lease(sec)  Type           VLAN  Interface
-----
00-01-01-01-01-01 10.1.1.10      infinite   static         100   eth1/0/3
00-01-01-01-01-10 10.1.1.11      3120      dhcp-snooping 100   eth1/0/3

Total Entries: 2

Switch#
```

В данном примере показано, как настроить отображение привязки IP Source Guard для IP-адреса 10.1.1.10.

```
Switch# show ip source binding 10.1.1.10

MAC Address      IP Address      Lease(sec)  Type           VLAN  Interface
-----
00-01-01-01-01-01 10.1.1.10      infinite   static         100   eth1/0/3

Total Entries: 1

Switch#
```

В данном примере показано, как настроить отображение привязки IP Source Guard для IP-адреса 10.1.1.11, MAC-адреса 00-01-01-01-01-10 в VLAN 100 на Ethernet 1/0/3 и изучение DHCP Snooping.

```
Switch# show ip source binding 10.1.1.10 00-01-01-01-01-10 dhcp-snooping vlan 100 interface eth1/0/3

MAC Address      IP Address      Lease(sec)  Type           VLAN  Interface
-----
00-01-01-01-01-10 10.1.1.11      3564      dhcp-snooping 100   eth1/0/3

Total Entries: 1

Switch#
```

Отображаемые параметры

MAC Address	MAC-адрес клиента.
IP Address	IP-адрес клиента, назначенный DHCP-сервером или настроенный пользователем.
Lease (sec)	Время аренды IP-адреса.
Type	Тип привязки. Статическая привязка настраивается вручную. Динамическая привязка изучается с помощью DHCP Snooping.
VLAN	Номер VLAN, где находится интерфейс клиента.
Interface	Интерфейс, подключаемый к узлу DHCP-клиента.

44-4 show ip verify source

Данная команда используется для отображения записи списка управления доступом (ACL) аппаратного порта на определенном интерфейсе.

show ip verify source [interface *INTERFACE-ID*] [, | -]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите порт или диапазон портов для настройки.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения записей списка управления доступом (ACL) аппаратного порта на определенном интерфейсе в таблице оборудования.

Пример

В данном примере показано, как настроить отображение, когда включен DHCP Snooping в VLAN 100 – 110, интерфейс в режиме IP Source Filter Mode настроен как IP, существующая привязка произведена к порту 10.1.1.1 в VLAN 100.

```
Switch#show ip verify source interface ethernet 1/0/3

Interface      Filter-type  Filter-mode  IP address    MAC address    VLAN
-----      -
eth1/0/3      ip          active      10.1.1.1     -              100
eth1/0/3      ip          active      deny-all    -              101-120

Total Entries: 2

Switch#
```

В данном примере показано, как настроить отображение, если интерфейс в режиме IP Source Filter Mode настроен как IP MAC, существующая привязка IP MAC привязывает IP-адрес 10.1.1.10 к MAC-адресу 00-01-01-01-01-01 в VLAN 100 и IP-адрес 10.1.1.11 к MAC-адресу 00-01-01-01-01-10 в VLAN 101.

```
Switch# show ip verify source interface eth1/0/3

Interface      Filter-type  Filter-mode  IP address      MAC address      VLAN
-----      -
eth1/0/3      ip-mac       active       10.1.1.10      00-01-01-01-01-01  100
eth1/0/3      ip-mac       active       10.1.1.11      00-01-01-01-01-10  101
eth1/0/3      ip-mac       active       deny-all      -                 102-120

Total Entries: 3

Switch#
```

Отображаемые параметры

Interface	Интерфейс, на котором включен IP Inspection.
Filter-type	Тип действующего IP Source Guard. ip: для авторизации IP-пакетов используется только IP-адрес. ip-mac: для авторизации IP-пакетов используется IP и MAC-адрес.
Filter-Mode	Active: активная проверка записей IP Source. inactive-trust-port: включить DHCP Snooping для доверенных портов без активной проверки записей IP Source. inactive-no-snooping-vlan: не настроено DHCP Snooping в VLAN, нет активной проверки записей IP Source.
IP address	IP-адрес клиента, назначенный DHCP-сервером или настроенный пользователем
MAC address	MAC-адрес клиента.
VLAN	Номер VLAN интерфейса клиента.

45. Команды IP Utility

45-1 ping

Данная команда используется для диагностики базового сетевого соединения.

```
ping {[ip] IP-ADDRESS | [ipv6] IPV6-ADDRESS | HOST-NAME} [length LENGTH] [count TIMES][timeout SECONDS] [source {IP ADDRESS | IPV6-ADDRESS}]
```

Параметры

ip <i>IP-ADDRESS</i>	(Опционально) Укажите, чтобы использовать IPv4-адрес. Укажите IPv4-адрес узла назначения (destination).
ipv6 <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.
length <i>LENGTH</i>	(Опционально) Укажите количество байтов данных, которое необходимо отправить. Значение не включает длину тега VLAN или IEEE 802.1Q. Доступный диапазон значений: от 1 до 1420.
count <i>TIMES</i>	(Опционально) Укажите, чтобы завершить процесс после отправки указанного количества пакетов Echo Request.
timeout <i>SECONDS</i>	(Опционально) Укажите время ожидания ответа в секундах.
source { <i>IP ADDRESS</i> <i>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 **length** – 56 байт.

Параметр **count** отключен.

Ping будет продолжаться до тех пор, пока пользователь не завершит процесс.

Значение **timeout** – 1 секунда.

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы проверить доступность, надежность и задержку маршрута к узлу назначения. Если не выбран параметр **count** или **timeout**, остановить Ping можно только используя комбинацию клавиш Ctrl+C.

Пример

В данном примере показано, как протестировать узел с IP-адресом 172.50.71.123.

```
Switch#ping 172.50.71.123 count 5

Reply from 172.50.71.123, time<10ms
Reply from 172.50.71.123, time<10ms
Reply from 172.50.71.123, time<10ms
Reply from 172.50.71.123, time<10ms
Reply from 172.50.71.123, time<10ms

Ping Statistics for 172.50.71.123
Packets: Sent =5, Received =5, 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 count 3

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 =3, Received =3, Lost =0

Switch#
```

45-2 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать список доступа, который ограничит доступ для Ping.

Пример

В данном примере показано, как создать стандартный список доступа IP и указать его как список доступа, который ограничит для Ping. Тестировать коммутатор разрешено только узлу 226.1.1.1.

```
Switch# configure terminal
Switch(config)# ip access-list ping-filter
Switch(config-ip-acl)# permit 226.1.1.1 0.0.0.0
Switch(config-ip-acl)# exit
Switch(config)# ping access-class ping-filter
Switch(config)#
```

45-3 traceroute

Данная команда используется для отображения пути передачи от узла к узлу через сеть IP от коммутатора к указанному узлу назначения (destination).

traceroute **{[ip] IP-ADDRESS | [ipv6] IPV6-ADDRESS | HOST-NAME}** **[length LENGTH] [probe NUMBER]**
[timeout SECONDS] [max-ttl TTL] [port DEST-PORT]

Параметры

ip	(Опционально) Укажите, чтобы использовать IPv4-адрес.
IP-ADDRESS	Укажите IPv4-адрес узла назначения.
ipv6	(Опционально) Укажите, чтобы использовать IPv6-адрес.
IPV6-ADDRESS	Укажите IPv6-адрес системы, который необходимо обнаружить.
HOST-NAME	Укажите имя узла системы, которое необходимо обнаружить.
Probe NUMBER	(Опционально) Укажите количество дейтаграмм, которое необходимо отослать. Доступный диапазон значений: от 1 до 1000.
timeout SECONDS	(Опционально) Укажите время ожидания ответа в секундах.
max-ttl TTL	(Опционально) Укажите максимальное значение TTL для исходящих UDP-дейтаграмм. Максимальный доступный диапазон значений: от 1 до 255.
port DEST-PORT	(Опционально) Укажите количество базовых UDP-портов назначения, используемых в исходящих дейтаграммах. Значение увеличивается при отправке каждой

дейтаграммы. Допустимый диапазон для порта назначения: от 1 до 65535. Используйте данную опцию в маловероятных событиях, если узел назначения прослушивает порт в диапазоне портов Trace Route по умолчанию.

По умолчанию

По умолчанию отправляются три 40-байтовые UDP-дейтаграммы, Initial TTL которых равен 1. Максимальное значение TTL – 30. Значение **timeout** – 5 секунд. Количество базовых UDP-портов назначения – 33434. Количество запросов для каждого TTL – 3.

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Чтобы прервать выполнение данной команды, используйте сочетание клавиш Ctrl+C.

Данная команда использует поле TTL в IP-заголовке, чтобы маршрутизаторы и серверы могли генерировать определенные ответные сообщения (Return messages). **Traceroute** запускается при отправке UDP-дейтаграммы на узел назначения с полем TTL 1. Если маршрутизатор обнаруживает значение TTL 1 или 0, дейтаграмма будет отброшена, а отправителю будет выслано ответное сообщение об истечении времени ответа (ICMP Time Exceeded). **Traceroute** определяет адрес первого узла при проверке поля адреса источника (source) сообщения ICMP Time Exceeded.

Чтобы идентифицировать следующий узел, **traceroute** снова отправляет UDP-пакет, но в этот раз значение TTL равно 2. Первый маршрутизатор уменьшает поле TTL на 1 и отправляет дейтаграмму на следующий маршрутизатор. Обнаружив TTL со значением 1, второй маршрутизатор отбрасывает дейтаграмму и отправляет на источник сообщение Time Exceeded. Этот процесс продолжается до тех пор, пока значение TTL не увеличится настолько, чтобы дейтаграмма могла достичь узла назначения (или до тех пор, пока не будет достигнуто максимальное значение TTL).

Чтобы определить, достигла ли дейтаграмма своего назначения, **traceroute** устанавливает очень большое значение для UDP-порта назначения в дейтаграмме, так что оно вряд ли будет использоваться узлом назначения. Если узел получает дейтаграмму с нераспознанным номером порта, на источник будет отправлена ошибка ICMP Port Unreachable. Данное сообщение свидетельствует **traceroute** о том, что дейтаграмма достигла назначения.

Пример

В данном примере показано, как выполнить трассировку маршрута к узлу 172.50.71.123.


```
Switch# traceroute 172.50.71.123
<10 ms 172.50.71.123
Trace complete.
Switch#
```

В данном примере показано, как выполнить трассировку маршрута к узлу 172.50.71.123, при этом маршрутизатор не отвечает.

```
Switch# traceroute 172.50.71.123
*      Request timed out.
*      Request timed out.
Switch#
```

В данном примере показано, как выполнить трассировку маршрута к узлу 172.50.71.123, при этом маршрутизатор отвечает, что назначение недоступно.

```
Switch# traceroute 172.50.71.123
<10 ms Network Unreachable
Switch#
```

В данном примере показано, как выполнить трассировку маршрута к узлу с IPv6-адресом 2001:238:f8a:77:7c10:41c0:6ddd:ecab.

```
Switch# traceroute 2001:238:f8a:77:7c10:41c0:6ddd:ecab
<10 ms 2001:238:f8a:77:7c10:41c0:6ddd:ecab
Trace complete.
Switch#
```

45-4 ip helper-address

Данная команда используется для того, чтобы добавить адрес назначения для передачи пакетов UDP Broadcast. Используйте форму **no**, чтобы удалить адрес назначения передачи.

```
ip helper-address IP-ADDRESS
no ip helper-address [IP-ADDRESS]
```

Параметры

<i>IP-ADDRESS</i>	Укажите IP-адрес назначения для передачи пакетов UDP Broadcast.
-------------------	---

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для конфигурирования интерфейса VLAN. Используйте данную команду, чтобы контролировать передачу пакетов UDP Broadcast. Команда действует только в том случае, если полученному интерфейсу присвоен IP-адрес.

Система передает только те пакеты, которые соответствуют следующим требованиям:

- MAC-адрес назначения (destination) должен быть широковещательным адресом.
- IP-адрес назначения должен быть широковещательным адресом.
- Тип пакетов – IPv4 UDP.
- Значение IP TTL должно быть больше или равно 2.

Пример

В данном примере показано, как сконфигурировать адрес IP Helper для VLAN 100. Указанный адрес – 172.50.71.123.

```
Switch# configure terminal
Switch(config)#interface vlan 100
Switch(config-if)#ip helper-address 172.50.71.123
Switch(config-if)#
```

45-5 ip forward-protocol

Данная команда используется для включения передачи пакетов UDP определенного типа службы. Используйте форму **no**, чтобы отключить передачу пакетов UDP определенного типа службы.

```
ip forward-protocol udp [PORT]
no ip forward-protocol udp [PORT]
```

Параметры

<i>PORT</i>	(Опционально) Укажите порт назначения (destination), на который необходимо передать / нельзя передать пакеты UDP определенного типа службы.
-------------	---

По умолчанию

По умолчанию включены часто используемые протоколы приложений.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Ниже представлен список часто используемых протоколов приложений, которые будут переданы по умолчанию, если адрес IP Helper сконфигурирован. Если команда или форма по данной команды сконфигурирована без указания номера порта, будут применены порты по умолчанию. Порт 67 и порт 68 BOOTP UDP указать нельзя, так как пакеты передаются при помощи DHCP Relay. Ниже перечислены порты по умолчанию:

- Порт 69 Trivial File Transfer Protocol (TFTP).
- Порт 53 Domain Naming System (DNS).
- Порт 37 Time service.
- Порт 137 NetBIOS Name Server.
- Порт 138 NetBIOS Datagram Server.
- Порт 49 TACACS service.
- Порт 42 IEN-116 Name Service.

Пример

В данном примере показано, как настроить адрес IP Helper для VLAN 100. Указанный адрес – 172.50.71.123. Передача адреса IP Helper на порту 53 UDP (DNS) отключена.

```
Switch# configure terminal
Switch(config)# interface vlan 100
Switch(config-if)# ip helper-address 172.50.71.123
Switch(config-if)# exit
Switch(config)# no ip forward-protocol udp 53
Switch(config)#
```

45-6 show ip helper-address

Данная команда используется для отображения таблицы адресов UDP Helper.

show ip helper-address [INTERFACE-ID]

Параметры

<i>INTERFACE-ID</i>	(Опционально) Укажите VLAN interface ID, который необходимо отобразить. Если interface ID не указан, будет отображена информация для всех интерфейсов.
---------------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить таблицу адресов UDP Helper.

Пример

В данном примере показано, как отобразить таблицу адресов UDP Helper.

```
Switch#show ip helper-address
```

```
Interface  Helper-address
```

```
-----  -
```

```
vlan 200  10.0.2.15
```

```
vlan 400  1.1.1.3
```

```
1.1.1.4
```

```
1.1.1.5
```

```
1.1.1.6
```

```
1.1.1.7
```

```
1.1.1.8
```

```
1.1.1.9
```

```
1.1.1.10
```

```
1.1.1.11
```

```
1.1.1.12
```

```
1.1.1.13
```

```
1.1.1.14
```

```
1.1.1.15
```

```
1.1.1.16
```

```
1.1.1.17
```

```
1.1.1.18
```

```
1.1.1.19
```

```
1.1.1.20
```

```
30.90.90.88
```

```
Switch#
```

45-7 show ip forward-protocol udp

Данная команда используется для отображения информации обо всех указанных UDP-портах.

```
show ip forward-protocol udp
```

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию обо всех указанных UDP-портах.

Пример

В данном примере показано, как отобразить информацию обо всех указанных UDP-портах.

```
Switch#show ip forward-protocol udp

Application          UDP Port
-----
Time Service        37
IEN-116 Name Service 42
TACACS              49
TFTP                69
NetBIOS-NS         137
NetBIOS-DS         138

Switch#
```

46. Команды IP-MAC-Port Binding (IMPВ)

46-1 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

all	Укажите для удаления всех неразрешенных записей.
interface <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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

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#
```

46-2 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.
-------------	---

strict-mode: укажите для включения строгого режима управления доступом (strict).

loose-mode: укажите для включения режима управления доступом loose. Если режим не задан, используется **strict-mode**.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если на порту назначен режим управления доступом IMPB **strict-mode**, узел может получить доступ к порту только после того, как узел отправит ARP или IP-пакеты, и эти пакеты пройдут проверку привязки. Чтобы пройти проверку привязки, IP и MAC-адрес источника, VLAN ID и номер порта назначения должны совпадать с любой записью, определенной либо статической записью привязки IP Source Guard, либо изученной динамической записью привязки DHCP Snooping.

Если на порту назначен режим управления доступом IMPB **loose-mode**, узлу будет отказано в доступе к порту после отправки узлом ARP или IP-пакетов, а эти пакеты, отправленные узлом, не пройдут проверку привязки. Чтобы пройти проверку привязки, IP и MAC-адрес источника, VLAN ID и номер порта назначения должны совпадать с любой записью, определенной либо статической записью привязки IP Source Guard, либо изученной динамической записью привязки DHCP Snooping.

Пример

В данном примере показано, как включить управление доступом IMPB на Ethernet 1/0/10.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/10
Switch(config-if)# ip ip-mac-port-binding strict
Switch(config-if)#
```

46-3 show ip ip-mac-port-binding

Данная команда используется для отображения настроек IMPB или записей, заблокированных с помощью управления доступом IMPB.

show ip ip-mac-port-binding [interface *INTERFACE-ID* [, | -]] [violation]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите для отображения определенного интерфейса.
--------------------------------------	---

,	(Опционально) Выделение серии интерфейсов или
---	---

	разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
violation	(Опционально) Укажите для отображения заблокированной записи.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

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#
```

46-4 snmp-server enable traps ip-mac-port-binding

Данная команда используется для включения уведомлений SNMP для привязки IP-MAC-Port Binding. При использовании формы **no** команда отключит уведомления SNMP.

```
snmp-server enable traps ip-mac-port-binding
no snmp-server enable traps ip-mac-port-binding
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

При включении данной функции коммутатор будет отправлять трапы при нарушениях безопасности, если будет получен некорректный пакет. Используйте эту команду для включения или отключения отправки уведомлений SNMP для таких событий.

Пример

В данном примере показано, как включить отправку трапов для IP-MAC-Port Binding.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps ip-mac-port-binding
Switch(config)#
```

47. Команды IPv6 Snooping

47-1 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

По умолчанию ни одной политики IPv6 Snooping Policy не создано.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для создания политики IPv6 Snooping Policy и входа в режим IPv6 Snooping Configuration Mode. После создания политики IPv6 Snooping используйте команду **ipv6 snooping attach-policy** для применения политики на указанном интерфейсе.

Пример

В данном примере показано, как создать политику IPv6 Snooping с именем policy1.

```
Switch# configure terminal
Switch(config)#ipv6 snooping policy policy1
Switch(config-ipv6-snooping)#
```

47-2 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 | dhcp-pd}
no protocol {dhcp | ndp | dhcp-pd}
```

Параметры

dhcp	Укажите для отслеживания адресов DHCPv6-пакетов.
ndp	Укажите для отслеживания адресов NDP-пакетов.
dhcp-pd	Укажите для отслеживания префикса IPv6 DHCPv6 PD-пакетов.

По умолчанию

По умолчанию все протоколы отключены.

Режим ввода команды

IPv6 Snooping Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Функция Neighbor Discovery (ND) Snooping создана для автонастройки адресов IPv6 без аутентификации и адресов IPv6, настроенных вручную. Перед назначением адреса IPv6, узел должен сначала выполнить Duplicate Address Detection (DAD). ND Snooping обнаруживает сообщения DAD, включающие DAD Neighbor Solicitation (NS) и DAD Neighbor Advertisement (NA), для построения таблицы привязки. NDP-пакет (NS и NA) также используется для определения того, доступен ли узел по-прежнему и можно ли удалить привязку или нет.

DHCPv6 Snooping анализирует DHCPv6-пакеты, отправляемые между DHCPv6-клиентом и сервером во время процедуры назначения адреса. Когда DHCPv6-клиент успешно получает корректный IPv6-адрес, DHCPv6 Snooping создает его таблицу привязки.

DHCP-PD Snooping анализирует пакеты DHCPv6 Prefix Delegation (PD) между Delegating Router (назначенным IPv6-префиксом) и соответствующим Requesting Router для настройки привязки префикса.

Пример

В данном примере показано, как включить DHCPv6 Snooping.

```
Switch# configure terminal
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# protocol dhcp
Switch(config-ipv6-snooping)#
```

47-3 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 1024.

По умолчанию

По умолчанию ограничений нет.

Режим ввода команды

IPv6 Snooping Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для ограничения количества привязок IPv6 Snooping, для которых применяется политика IPv6 Sooring Policy. Команда помогает ограничить размер таблицы привязки.

Пример

В данном примере показано, как задать максимальное число 25 для привязки IPv6 Snooping.

```
Switch# configure terminal
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# limit address-count 25
Switch(config-ipv6-snooping)#
```

47-4 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

По умолчанию политика IPv6 Snooping Policy не применяется.

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

После создания политики IPv6 Snooping Policy используйте данную команду для применения политики к определенной VLAN.

Пример

В данном примере показано, как создать включить IPv6 Snooping в VLAN 200.

```
Switch#configure terminal
Switch(config)#vlan 200
Switch(config-vlan)#ipv6 snooping attach-policy policy1
Switch(config-vlan)#
```

47-5 ipv6 snooping station-move deny

Данная команда используется для запрета функции Station Move для привязки IPv6 Snooping. При использовании формы **no** данная команда вернется к значениям по умолчанию.

```
ipv6 snooping station-move deny
no ipv6 snooping station-move deny
```

Параметры

Нет

По умолчанию

По умолчанию функция Station Move разрешена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Когда функция Station Move разрешена, динамическая запись привязки Snooping с тем же VLAN ID и MAC-адресом на указанном порту может продвинуться к другому порту, если обнаружены следующие условия:

- Запись привязки DHCPv6 Snooping запускает новый DHCP-процесс на новом интерфейсе.
- Запись привязки ND Snooping запускает новый DAD-процесс на новом интерфейсе.

Пример

В данном примере показано, как запретить функцию Station Move.

```
Switch# configure terminal
Switch(config)# ipv6 snooping station-move deny
Switch(config)#
```

47-6 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

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для просмотра информации о DHCPv6 Guard. Если параметр не указан, отображаться будет информация для всех политик.

Пример

В данном примере показано, как включить отображение информации о DHCPv6 Guard.

```
Switch#show ipv6 snooping policy
```

```
Snooping policy: policy1
  Protocol: DHCP
  Limit Address Count: 25
  Target VLAN: 200
```

```
Switch#
```

Отображаемые параметры

Protocol	Протокол, используемый для Snooping.
Limit Address Count	Максимально допустимое число записей для данной политики IPv6 Snooping Policy.
Target VLAN	Имя списка VLAN.

48. Команды IPv6 Source Guard

48-1 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для добавления статической записи в таблицу привязки вручную. Для данной команды указанная VLAN необязательно должна существовать. Если указанный интерфейс позже будет удален, настройки команды будут соответственно также удалены.

Пример

В данном примере показано, как настроить привязку IPv6 Source Guard с адресом IPv6 2000::1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 на Ethernet 1/0/10.

```
Switch# configure terminal
Switch(config)# ipv6 source binding 00-01-02-03-04-05 vlan 2 2000::1 interface ethernet 1/0/10
Switch(config)#
```

48-2 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для создания политики IPv6 Source Guard Policy. Команда позволяет войти в режим IPv6 Source-Guard Policy Configuration Mode.

Пример

В данном примере показано, как создать политику IPv6 Source Guard Policy.

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy policy1
Switch(config-source-guard)#
```

48-3 deny global-autoconfig

Данная команда используется для запрета автоматически сконфигурированного трафика. При использовании формы **no** команда отключит данную функцию.

deny global-autoconfig
no deny global-autoconfig

Параметры

Нет

По умолчанию

По умолчанию данная опция разрешена.

Режим ввода команды

Source-Guard Policy Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для запрета трафика от автоматически сконфигурированных глобальных адресов. Она может использоваться, когда все глобальные адреса назначены DHCP, и администратор хочет заблокировать входящий трафик от узлов с самостоятельно сконфигурированными адресами.

Пример

В данном примере показано, как запретить автоматически сконфигурированный трафик.

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy policy1
Switch(config-source-guard)# deny global-autoconfig
Switch(config-source-guard)#
```

48-4 permit link-local

Данная команда используется для аппаратного разрешения трафика данных, отправленного с адреса Link-Local. При использовании формы **no** команда отключит данную функцию.

permit link-local
no permit link-local

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Source-Guard Policy Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для аппаратного разрешения трафика данных, отправленного с адреса 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)#
```

48-5 validate address

Данная команда используется для включения функции IPv6 Source Guard для выполнения проверки адреса. При использовании формы **no** команда отключит функцию проверки адреса.

validate address
no validate address

Параметры

Нет

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Source-Guard Policy Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения функции IPv6 Source Guard для выполнения проверки адреса.

Пример

В данном примере показано, как отключить функцию проверки адреса.

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy policy1
Switch(config-source-guard)# no validate address
Switch(config-source-guard)#
```

48-6 validate prefix

Данная команда используется для включения функции IPv6 Source Guard для выполнения операции защиты IPv6 Prefix-Guard. При использовании формы **no** команда отключит данную функцию.

validate prefix
no validate prefix

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Source-Guard Policy Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения функции IPv6 Source Guard для выполнения операции защиты IPv6 Prefix-Guard.

Пример

В данном примере показано, как включить функцию IPv6 Source Guard для выполнения операции защиты IPv6 Prefix-Guard.

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy policy1
Switch(config-source-guard)# validate prefix
Switch(config-source-guard)#
```

48-7 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

<i>POLICY-NAME</i>	(Опционально) Укажите имя политики Source Guard Policy.
--------------------	---

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Когда команда применена к порту, принятый IPv6-пакет, кроме ND, RA, RS и DHCP-сообщений будет выполнять проверку привязки адреса. Пакет будет разрешен, если он соответствует любой записи в таблице привязки адресов. Таблица привязки включает в себя динамическую таблицу (созданную с помощью команд IPv6 Snooping) и статическую таблицу (созданную с помощью команды **ipv6 source binding vlan**).

Если имя политики не указано, по умолчанию политика Source Guard Policy разрешит пакеты, отправленные с помощью автоматически сконфигурированного адреса, и запретит пакеты, отправленные с адреса Link-Local.

Пример

В данном примере показано, как применить политику IPv6 Source Guard Policy «pol1» на Ethernet 1/0/3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ipv6 source-guard attach-policy poll
Switch(config-if)#
```

48-8 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

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для просмотра настроек IPv6 Source Guard Policy. Если имя политики не указано, отображаться будет информация для всех политик IPv6 Source Guard.

Пример

В данном примере показано, как включить отображение настроек для IPv6 Source Guard Policy.

```
Switch#show ipv6 source-guard policy

Policy policy1 configuration:
  Target: eth1/0/3

Switch#
```

48-9 show ipv6 neighbor binding

Данная команда используется для просмотра таблицы привязки IPv6.

```
show ipv6 neighbor binding [vlan VLAN-ID] [interface INTERFACE-ID] [ipv6 IPV6-ADDRESS][mac MAC-ADDRESS]
```

Параметры

vlan <i>VLAN-ID</i>	(Опционально) Укажите для отображения привязок, соответствующих указанной VLAN.
interface <i>INTERFACE-ID</i>	(Опционально) Укажите для отображения привязок, соответствующих указанному номеру интерфейса.
ipv6 <i>IPV6-ADDRESS</i>	(Опционально) Укажите для отображения привязок, соответствующих указанному адресу IPv6.
mac <i>MAC-ADDRESS</i>	(Опционально) Укажите для отображения привязок, соответствующих указанному MAC-адресу.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Команда используется для просмотра 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, P - DHCP-PD Snooping
 IPv6 address      MAC address      Interface      VLAN Time left
S 1000::1          000D.8811.8B6A  eth1/0/2      1    N/A
N FE80::A8BB:CCFF:FE01:F500  A8BB.CC01.F500 eth1/0/3      100  8850
S FE80::21D:71FF:FE99:4900  001D.7199.4900 eth1/0/4      100  N/A
N 2001:600::1      A8BB.CC01.F500 eth1/0/5      100  3181
D 2001:100::2      A8BB.CC01.F600 eth1/0/6      200  9196
D 2001:400::1      001D.7199.4900 eth1/0/7      100  1568
S 2001:500::1      000A.000B.000C eth1/0/8      300  N/A
P 400::/64                    eth1/0/9      300  1440

Total Entries: 8

Switch#
```

Отображаемые параметры

Codes	Коды для IPv6 Snooping Owner D: DHCPv6 Snooping S: Статический N: ND Snooping
IPv6 address	IPv6-адрес привязки.
MAC address	MAC-адрес привязки.
Interface	Номер интерфейса привязки.
VLAN	VLAN привязки.
Time left	Оставшееся время жизни привязки. Период отсутствия активности для статической привязки.

49. Команды Jumbo Frame

49-1 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

<i>BYTES</i>	Укажите максимально допустимый размер Ethernet-фреймов. Доступный диапазон значений: от 64 до 12288 байт.
--------------	--

По умолчанию

Значение по умолчанию – 1536 байт.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для конфигурирования физических портов. Фреймы избыточного размера будут отброшены, на входных портах будут проведены проверки. Используйте данную команду, чтобы передавать большие фреймы или jumbo-фреймы через коммутатор и оптимизировать передачу от сервера к серверу.

Пример

В данном примере показано, как настроить максимальный размер полученных Ethernet-фреймов на порту 1/0/3. Указанное значение – 6000 байт.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/3
Switch(config-if)#max-rcv-frame-size 6000
Switch(config-if)#
```

50. Команды Layer 2 Protocol Tunnel (L2PT)

50-1 clear l2protocol-tunnel counters

Данная команда используется для обнуления счетчиков статистики L2PT (Layer 2 Protocol Tunnel).

```
clear l2protocol-tunnel counters {all | interface INTERFACE-ID}
```

Параметры

all	Укажите, чтобы обнулить счетчики для всех интерфейсов.
interface <i>INTERFACE-ID</i>	Укажите интерфейс, для которого необходимо обнулить счетчики.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы обнулить счетчики Protocol Tunnel для всех интерфейсов или для указанного интерфейса. Доступны только физические порты и port-channel.

Пример

В данном примере показано, как обнулить счетчики L2PT для всех портов L2PT.

```
Switch# clear l2protocol-tunnel counters all
Switch#
```

50-2 l2protocol-tunnel

Данная команда используется для того, чтобы включить туннелирование для указанных протоколов. Используйте форму **no**, чтобы отключить данную функцию.

```
l2protocol-tunnel [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]
no l2protocol-tunnel [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]
```

Параметры

gvrp	(Опционально) Укажите, чтобы включить туннелирование для пакетов GVRP (GARP VLAN Registration Protocol).
-------------	--

stp	(Опционально) Укажите, чтобы включить туннелирование для пакетов STP (Spanning Tree Protocol).
01-00-0c-cc-cc-cc	(Опционально) Укажите адрес назначения (destination) пакетов протокола, которые необходимо туннелировать.
01-00-0c-cc-cc-cd	(Опционально) Укажите адрес назначения пакетов протокола, которые необходимо туннелировать.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить функцию L2PT. Данная функция позволяет обмениваться информацией о работе протокола на локальном и удаленном сайте через сеть поставщика услуг. Если тип протокола не указан, команда запускает туннелирование всех типов протоколов.

Сконфигурировать L2PT для протокола GVRP/STP на порту можно вне зависимости от того, включен ли GVRP/STP. Однако если для GVRP/STP включена функция L2PT, функционирование протокола GVRP/STP на порту будет невозможно.

Если пакет L2-протокола прибывает на порт, на котором включено туннелирование протокола, коммутатор классифицирует пакет с сервисной VLAN и передает пакет на порты-члены сервисной VLAN. Обычно пакет инкапсулируется и передается на удаленный сайт через trunk-порт. При передаче пакета на удаленный сайт через trunk-порт туннелированный пакет будет тегирован с сервисной VLAN. Пакет также может быть передан на другие порты локального сайта, на которых включена функция туннелирования протокола.

Обычно туннелирование протокола инкапсулирует пакет протокола, заменяя MAC-адрес назначения пакета на заданный vendor-ом групповой адрес. Однако если на порту передачи включена функция L2PT, MAC-адрес назначения пакета протокола не будет изменен.

На удаленном сайте коммутатор деинкапсулирует туннелированный пакет, восстанавливая заданный vendor-ом групповой адрес до изначального PDU-адреса, и передает пакет на клиентскую сеть через порты, на которых включено туннелирование протокола.

Если порт, на котором включена функция L2PT, получит инкапсулированный пакет, порт перейдет в состояние «отключено из-за ошибки».

Пример

В данном примере показано, как включить функцию L2PT для STP-протокола на интерфейсе.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# l2protocol-tunnel stp

WARNING: STP doesn't run when l2 protocol tunnel is enabled for the port.

Switch(config-if)#
```

50-3 l2protocol-tunnel cos

Данная команда используется для того, чтобы указать значение CoS для L2PT. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
l2protocol-tunnel cos COS-VALUE
no l2protocol-tunnel cos
```

Параметры

<i>COS-VALUE</i>	Укажите значение CoS в диапазоне от 0 до 7. Высший приоритет - 7.
------------------	---

По умолчанию

Значение по умолчанию – 5.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если пакет L2-протокола прибывает на порт, на котором включена функция L2PT, коммутатор инкапсулирует пакет с тегом сервисной VLAN и заменяет значение CoS на значение, указанное при помощи данной команды.

Пример

В данном примере показано, как указать значение CoS для L2PT.

```
Switch# configure terminal
Switch(config)# l2protocol-tunnel cos 7
Switch(config)#
```

50-4 l2protocol-tunnel drop-threshold

Данная команда используется для того, чтобы указать пороговое количество пакетов L2-протокола, полученных на порту. Пакеты, полученные после превышения заданного значения, будут отброшены. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```

l2protocol-tunnel drop-threshold [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-
cd}] PPS
no l2protocol-tunnel drop-threshold [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-
cc-cd}]

```

Параметры

gvrp	(Опционально) Укажите GVRP-пакеты.
stp	(Опционально) Укажите STP-пакеты.
01-00-0c-cc-cc-cc	(Опционально) Укажите адрес назначения (destination) пакетов протокола.
01-00-0c-cc-cc-cd	(Опционально) Укажите адрес назначения пакетов протокола.
<i>PPS</i>	Укажите пороговое значение по количеству пакетов в секунду. Доступный диапазон значений: от 1 до 4096.

По умолчанию

По умолчанию пороговое значение не задано.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

При инкапсулировании, декапсулировании и передаче пакетов функцией L2PT расходуется производительность ЦПУ. Используйте данную команду, чтобы ограничить потребление производительности ЦПУ, указав пороговое количество пакетов L2-протокола, которое может быть получено на порту. Пакеты, полученные после превышения заданного значения, будут отброшены.

Если тип протокола не указан, настройки будут применены ко всем типам протоколов.

Используйте команду **l2protocol-tunnel drop-threshold** и команду **l2protocol-tunnel shutdown-threshold**, чтобы ограничить пропускную способность. Если на интерфейсе также сконфигурировано пороговое значение shutdown, пороговое значение drop должно быть меньше или равно указанному пороговому значению shutdown.

Пример

В данном примере показано, как сконфигурировать пороговое значение drop для STP-протокола.

```

Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# l2protocol-tunnel drop-threshold stp 2000
Switch(config-if)#

```

50-5 l2protocol-tunnel global drop-threshold

Данная команда используется для указания максимального количества пакетов L2-протокола, которое может быть обработано системой за 1 секунду. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
l2protocol-tunnel global drop-threshold PPS  
no l2protocol-tunnel global drop-threshold
```

Параметры

<i>PPS</i>	Укажите максимальное количество входящих пакетов L2-протокола, которое можно туннелировать. Допустимый диапазон значений: от 100 до 20000.
------------	--

По умолчанию

Пороговое значение по умолчанию не установлено.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

При инкапсулировании, декапсулировании и передаче пакетов L2-протокола функцией L2PT расходуется производительность ЦПУ. Используйте данную команду, чтобы ограничить потребление производительности ЦПУ, указав пороговое количество пакетов L2-протокола, которое может быть обработано системой. Пакеты, полученные после превышения заданного значения, будут отброшены.

Используйте команду **l2protocol-tunnel global drop-threshold** и команду **l2protocol-tunnel drop-threshold** в режиме Global Configuration Mode, чтобы ограничить пропускную способность.

Пример

В данном примере показано, как включить ограничение скорости передачи глобально.

```
Switch# configure terminal  
Switch(config)# l2protocol-tunnel global drop-threshold 5000  
Switch(config)#
```

50-6 l2protocol-tunnel shutdown-threshold

Данная команда используется для того, чтобы указать пороговое количество пакетов L2-протокола, полученных на порту. Пакеты, полученные после превышения заданного значения, будут отброшены. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
l2protocol-tunnel shutdown-threshold [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}] PPS
```

```
no l2protocol-tunnel shutdown-threshold [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]
```

Параметры

gvrp	(Опционально) Укажите GVRP-туннелирование.
stp	(Опционально) Укажите STP-туннелирование.
01-00-0c-cc-cc-cc	(Опционально) Укажите адрес назначения (destination) пакетов протокола.
01-00-0c-cc-cc-cd	(Опционально) Укажите адрес назначения пакетов протокола.
<i>PPS</i>	Укажите пороговое значение по количеству пакетов в секунду. Доступный диапазон значений: от 1 до 4096.

По умолчанию

Пороговое значение по умолчанию не установлено.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы ограничить потребление производительности ЦПУ, указав пороговое количество пакетов L2-протокола, которое может быть получено на порту. Если заданное пороговое значение превышено, порт перейдет в состояние «отключено из-за ошибки».

Если тип протокола не указан, настройки будут применены ко всем типам протоколов.

Используйте команду **l2protocol-tunnel shutdown-threshold** и команду **l2protocol-tunnel drop- threshold**, чтобы ограничить туннелирование. Если на интерфейсе также сконфигурировано пороговое значение drop, пороговое значение shutdown должно быть больше или равно указанному пороговому значению drop.

Пример

В данном примере показано, как указать максимальное количество STP-пакетов, которое может быть обработано на интерфейсе за 1 секунду.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# l2protocol-tunnel shutdown-threshold stp 200
Switch(config-if)#
```

50-7 l2protocol-tunnel mac-address

Данная команда используется для того, чтобы указать групповой адрес L2PT для обозначенного протокола. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```

l2protocol-tunnel mac-address [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]
MAC-ADDR
no l2protocol-tunnel mac-address [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]

```

Параметры

gvrp	(Опционально) Укажите GVRP-пакеты, которые необходимо туннелировать на обозначенный адрес.
stp	(Опционально) Укажите STP-пакеты, которые необходимо туннелировать на обозначенный адрес.
01-00-0c-cc-cc-cc	(Опционально) Укажите адрес назначения (destination) пакетов протокола, которые необходимо туннелировать на обозначенный адрес.
01-00-0c-cc-cc-cd	(Опционально) Укажите адрес назначения пакетов протокола, которые необходимо туннелировать на обозначенный адрес.
MAC-ADDR	Укажите MAC-адрес, на который необходимо туннелировать пакеты. Данный адрес не может быть зарезервирован или использован другими протоколами.

По умолчанию

Адрес туннелирования GVRP-пакетов – 01-05-5D-00-00-21.

Адрес туннелирования STP-пакетов – 01-05-5D-00-00-00.

Адрес туннелирования MAC-адреса 01-00-0C-CC-CC-CC протокола – 01-05-5D-00-00-10.

Адрес туннелирования MAC-адреса 01-00-0C-CC-CC-CD протокола – 01-05-5D-00-00-11.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать групповой адрес L2PT для обозначенного протокола. Если тип протокола не указан, настройки будут применены ко всем типам протоколов.

Ниже перечислены зарезервированные или используемые другими протоколами MAC-адреса, которые не могут быть сконфигурированы в команде:

- FF-FF-FF-FF-FF-FF
- 00-00-00-00-00-00
- Unicast MAC address
- 01-00-08-06-0F-0F
- 01-00-0C-CC-CC-CC
- 01-00-0C-CC-CC-CD
- 01-19-A7-00-00-01
- 01-1B-19-00-00-00

- от 01-80-C2-00-00-00 до 01-80-C2-00-00-0F
- 01-80-C2-00-00-10
- от 01-80-C2-00-00-20 до 01-80-C2-00-00-2F
- от 01-00-5E-00-00-00 до 01-00-5E-FF-FF-FF
- 33-33-00-00-00-04
- 33-33-00-00-00-05
- 33-33-00-00-00-06
- 33-33-00-00-00-09
- 33-33-00-00-00-0D
- CF-00-00-00-00-00

Пример

В данном примере показано, как указать групповой адрес L2PT для STP-протокола. Указанный адрес – 01-00-0ccd-cd-d0.

```
Switch#configure terminal
Switch(config)#l2protocol-tunnel mac-address stp 01-00-0c-cd-cd-d0
Switch(config)#
```

50-8 show l2protocol-tunnel

Данная команда используется для отображения протоколов, которые туннелированы на интерфейсе или на всех интерфейсах.

show l2protocol-tunnel [interface *INTERFACE-ID*]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите интерфейс, который необходимо отобразить.
--------------------------------------	---

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить настройки, статус и счетчики L2PT.

Пример

В данном примере показано, как отобразить туннелированные протоколы на всех интерфейсах.

```
Switch#show l2protocol-tunnel

CoS for Encapsulated Packets      :5
Drop Threshold for Encapsulated Packets :0

Protocol          Drop Counter   Tunneling Address
-----
gvrp              0              01-05-5D-00-00-21
stp              0              01-00-0C-CD-CD-00
01-00-0c-cc-cc-cc 0              01-05-5D-00-00-10
01-00-0c-cc-cc-cd 0              01-05-5D-00-00-11

Port      Protocol  Shutdown Drop      Encap  Decap  Drop
          Protocol Threshold Threshold Counter Counter Counter
-----
eth1/0/3  gvrp      -        2000    0       0       0
          stp      -        -        0       0       0
          01000ccccccc -        -        0       0       0
          01000ccccccd -        -        0       0       0
eth1/0/5  gvrp      -        2000    0       0       0
          stp      -        2000    0       0       0
          01000ccccccc -        2000    0       0       0
          01000ccccccd -        2000    0       0       0

Switch#
```

Отображаемые параметры

CoS for Encapsulated Packets	Значение CoS (Class of Service) для туннелированных пакетов L2-протокола.
Drop Threshold for Encapsulated Packets	Ограничение скорости на L2PT.
Protocol	Тип L2-протокола, который необходимо туннелировать.
Drop Counter	Количество отброшенных пакетов L2-протокола.
Tunneling Address	Настройки группового адреса туннелирования протокола.
Port	Порт, на котором включена функция L2PT.
Shutdown Threshold	Пороговое значение shutdown для указанного пакета L2-протокола.
Drop Threshold	Пороговое значение drop для указанного пакета L2-протокола.
Encap Counter	Количество пакетов L2-протокола, полученных и инкапсулированных портом, на котором включена функция L2PT.
Decap Counter	Количество пакетов L2-протокола, декапсулированных и переданных на порт, на котором включена функция L2PT.

51. Команды Link Aggregation Control Protocol (LACP)

51-1 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.
on	Укажите интерфейс в качестве статического участника channel-group.
active	Укажите, чтобы включить для интерфейса режим LACP Active Mode.
passive	Укажите, чтобы включить для интерфейса режим LACP Passive Mode.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для конфигурирования физических портов. При первом подключении порта к channel-group система автоматически создаст port-channel. Интерфейс может подключиться только к одной channel-group.

Если в команде указан параметр **on**, тип channel-group – статическая. Если в команде указан параметр **active** или **passive**, тип channel-group – LACP. Channel-group может состоять только или из статических участников, или из участников LACP. После того как тип channel-group был определен, интерфейсы других типов не смогут подключиться к channel-group.

Если на порту включена функция Security, данный порт нельзя указать в качестве участника channel-group.

Пример

В данном примере показано, как привязать интерфейсы от Ethernet 1/0/4 до Ethernet 1/0/5 к новой LACP channel-group с ID 3 и включить режим LACP Active Mode.

```
Switch# configure terminal
Switch(config)# interface range ethernet 1/0/4-1/0/5
Switch(config-if)# channel-group 3 mode active
Switch(config-if)#
```

51-2 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Приоритет порта LACP определяет, какие порты могут подключиться к port-channel и на каких портах включен режим Standalone Mode. Чем ниже значение, тем выше приоритет. Если у двух и более портов совпадает приоритет, то приоритет будет определяться номером порта.

Пример

В данном примере показано, как сконфигурировать приоритет порта на интерфейсах от Ethernet 1/0/4 до Ethernet 1/0/5. Указанное значение – 20000.

```
Switch# configure terminal
Switch(config)# interface range ethernet 1/0/4-1/0/5
Switch(config-if)# lacp port-priority 20000
Switch(config-if)#
```

51-3 lacp timeout

Данная команда используется для настройки таймера LACP Long или LACP Short. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
lacp timeout {short | long}
```

no lacp timeout

Параметры

short	Укажите, чтобы выбрать значение 3 секунды для интервала, по истечении которого полученная информация о LACPDU будет объявлена недействительной, и 1 секунду для интервала между регулярными передачами LACP PDU. Данный параметр применяется, если канал-партнер использует Short Timeouts.
long	Укажите, чтобы выбрать значение 90 секунд для интервала, по истечении которого полученная информация о LACPDU будет объявлена недействительной, и 30 секунд для интервала между регулярными передачами LACP PDU. Данный параметр применяется, если канал-партнер использует Long Timeouts.

По умолчанию

Режим LACP Timeout по умолчанию – Short.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для конфигурирования физических портов.

Пример

В данном примере показано, как сконфигурировать режим LACP Timeout Long на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lacp timeout long
Switch(config-if)#
```

51-4 lacp system-priority

Данная команда используется для настройки приоритета системы. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

lacp system-priority *PRIORITY*
no lacp system-priority

Параметры

PRIORITY

Укажите приоритет системы в диапазоне от 1 до 65535.

По умолчанию

Приоритет системы LACP по умолчанию – 32768.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Во время LACP-согласования локальный партнер обменивается с удаленным партнером приоритетом системы и приоритетом порта. При помощи приоритета порта коммутатор определяет, в каком режиме функционирует порт – Backup Mode или Active Mode. Приоритет системы LACP определяет коммутатор, контролирующий приоритет порта. Приоритеты портов других коммутаторов будут игнорированы.

Чем ниже значение, тем выше приоритет. Если у двух коммутаторов совпадает приоритет системы, приоритет будет определяться при помощи ID/MAC системы LACP. Команда приоритета системы LACP применима для всех LACP port-channel коммутатора.

Пример

В данном примере показано, как сконфигурировать приоритет системы LACP. Указанное значение – 30000.

```
Switch# configure terminal
Switch(config)# lacp system-priority 30000
Switch(config)#
```

51-5 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 | dst-l4-port |
src-dst-l4-port | src-l4 port}
no port-channel load-balance
```

Параметры

dst-ip	Укажите, чтобы коммутатор проверил IP-адрес назначения (destination).
dst-mac	Укажите, чтобы коммутатор проверил MAC-адрес назначения.
src-dst-ip	Укажите, чтобы коммутатор проверил IP-адрес источника (source) и IP-адрес назначения.
src-dst-mac	Укажите, чтобы коммутатор проверил MAC-адрес

	источника и MAC-адрес назначения.
src-ip	Укажите, чтобы коммутатор проверил IP-адрес источника.
src-mac	Укажите, чтобы коммутатор проверил MAC-адрес источника.
dst-l4-port	Укажите, чтобы коммутатор проверил TCP/UDP-порт назначения 4 уровня.
src-dst-l4-port	Укажите, чтобы коммутатор проверил TCP/UDP-порт источника 4 уровня и порт назначения 4 уровня.
src-l4 port	Укажите, чтобы коммутатор проверил TCP/UDP-порт источника 4 уровня.

По умолчанию

Алгоритм Load Balancing по умолчанию – **src-dst-mac**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать алгоритм Load Balancing. Можно указать только один алгоритм.

Пример

В данном примере показано, как сконфигурировать алгоритм Load Balancing src-ip.

```
Switch# configure terminal
Switch(config)# port-channel load-balance src-ip
Switch(config)#
```

51-6 show channel-group

Данная команда используется для отображения информации о channel-group.

show channel-group [channel [CHANNEL-NO] {detail | neighbor} | load-balance | sys-id]

Параметры

channel	(Опционально) Укажите, чтобы отобразить информацию для указанных port-channel.
CHANNEL-NO	(Опционально) Укажите channel-group ID.
detail	(Опционально) Укажите, чтобы отобразить подробную информацию о channel-group.
neighbor	(Опционально) Укажите, чтобы отобразить информацию о соседнем устройстве.
load-balance	(Опционально) Укажите, чтобы отобразить информацию о

	балансировке нагрузки.
sys-id	(Опционально) Укажите, чтобы отобразить system identifier, используемый LACP.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Если номер port-channel не указан, будут отображены все port-channel. Если в команде **show channel-group** не указаны параметры **channel**, **load-balance** и **sys-id**, будет отображена только краткая информация о channel-group.

Пример

В данном примере показано, как отобразить подробную информацию обо всех port-channel.

```
Switch#show channel-group channel detail

Flag:
  S - Port is requesting Slow LACPDU      F - Port is requesting fast LACPDU
  A - Port is in active mode              P - Port is in passive mode
LACP state:
  bndl:   Port is attached to an aggregator and bundled with other ports.
  hot-sby: Port is in a hot-standby state.
  indep:  Port is in an independent state(not bundled but able to switch data
          traffic)
  down:   Port is down.

Channel Group 3
Member Ports: 2, Maxports = 12, Protocol: LACP
Description:

```

Port	Flags	LACP State	Port Priority	Port Number
eth1/0/4	FA	down	20000	0
eth1/0/5	FA	down	20000	0

```
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          Partner  Partner  Partner
System ID    System ID        PortNo   Flags    Port_Pri
-----
eth1/0/21    32768,F0-7D-68-36-3C-00  21      FA       32768
eth1/0/22    32768,F0-7D-68-36-3C-00  22      FA       32768
eth1/0/23    0,00-00-00-00-00-00    0       SP       0
eth1/0/24    0,00-00-00-00-00-00    0       SP       0

Switch#
```

В данном примере показано, как отобразить информацию о балансировке нагрузки для всех channel-group.

```
Switch#show channel-group load-balance

load-balance algorithm: src-dst-mac

Switch#
```

В данном примере показано, как отобразить информацию о system identifier.

```
Switch#show channel-group sys-id

System-ID: 32768,F0-7D-68-34-00-10

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,F0-7D-68-34-00-10

Group      Protocol
-----
3          LACP

Switch#
```

52. Команды Link Layer Discovery Protocol (LLDP)

52-1 clear lldp counters

Данная команда используется для удаления статистики LLDP.

```
clear lldp counters [all | interface INTERFACE-ID [, | -]]
```

Параметры

all	(Опционально) Укажите, чтобы обнулить счетчик LLDP для всех интерфейсов и статистики Global LLDP.
interface <i>INTERFACE-ID</i>	(Опционально) Укажите интерфейс, на котором необходимо обнулить счетчик LLDP. Доступны только физические интерфейсы.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, указав параметр **interface**, чтобы сбросить счетчик статистики LLDP на выбранном интерфейсе/интерфейсах. Используйте команду **clear lldp counters**, указав параметр **all**, чтобы удалить статистику LLDP и Global LLDP на всех интерфейсах. Если не указаны дополнительные параметры, будут обнулены только счетчики Global LLDP.

Пример

В данном примере показано, как удалить всю статистику LLDP.

```
Switch# clear lldp counters all
Switch#
```

52-2 clear lldp table

Данная команда используется для удаления всей информации об LLDP, полученной от соседних устройств.

clear lldp table {all | interface *INTERFACE-ID* [, | -]}

Параметры

all	Укажите, чтобы удалить информацию об LLDP, полученную от соседних устройств, для всех интерфейсов.
<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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если в команде не указан параметр **interface**, будет удалена вся информация, полученная от соседних устройств, на всех интерфейсах.

Пример

В данном примере показано, как удалить всю информацию, полученную от соседних устройств, на всех интерфейсах.

```
Switch# clear lldp table all
Switch#
```

52-3 lldp dot1-tlv-select

Данная команда используется для указания дополнительных настроек TLV (type-length-value) в указанном в пределах IEEE 802.1 наборе TLV, которые будут переданы и инкапсулированы в LLDPDU, а затем отправлены на соседние устройства. Используйте форму **no**, чтобы отключить передачу TLV.

lldp dot1-tlv-select {port-vlan | protocol-vlan *VLAN-ID* [, | -] | vlan-name [*VLAN-ID* [, | -]] | protocol-identity [*PROTOCOL-NAME*]}
no lldp dot1-tlv-select {port-vlan | protocol-vlan [*VLAN-ID* [, | -]] | vlan-name [*VLAN-ID* [, | -]] | protocol-identity [*PROTOCOL-NAME*]}

Параметры

port-vlan	Укажите Port VLAN ID TLV, который необходимо отправить. Port VLAN ID TLV – это дополнительный TLV фиксированной длины, который позволяет порту VLAN Bridge анонсировать PVID (Port VLAN Identifier), который будет ассоциирован с нетегированными или тегированными по приоритету кадрами.
protocol-vlan	Укажите PPVID (Port and Protocol VLAN ID) TLV, который необходимо отправить. PPVID TLV – это дополнительный TLV, который позволяет порту Bridge анонсировать PPVID.
<i>VLAN-ID</i>	Укажите VLAN ID в PPVID TLV. Доступный диапазон значений: от 1 до 4094. Если VLAN ID не указан, все сконфигурированные PPVID VLAN будут удалены, PPVID TLV отправлен не будет.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
vlan-name	Укажите VLAN Name TLV, который необходимо отправить. VLAN Name TLV – это дополнительный TLV, который позволяет IEEE 802 LAN station, совместимой с IEEE 802.1Q, анонсировать присвоенное имя любой VLAN, с которой она сконфигурирована.
<i>VLAN-ID</i>	(Опционально) Укажите VLAN ID в VLAN Name TLV. Доступный диапазон значений: от 1 до 4094. Если VLAN ID не указан, все сконфигурированные VLAN для VLAN Name TLV будут удалены, VLAN Name TLV отправлен не будет.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
proto-col-identity	Укажите Protocol Identity TLV, который необходимо отправить. Protocol Identity TLV – это дополнительный TLV, который позволяет IEEE 802 LAN station анонсировать определенные протоколы, доступные через порт.
<i>PROTOCOL-NAME</i>	(Опционально) Укажите имя протокола. Ниже перечислены допустимые для <i>PROTOCOL-NAME</i> строки: eapol - Extensible Authentication Protocol (EAP) over LAN lACP - Link Aggregation Control Protocol gvrp - GARP VLAN Registration Protocol stp - Spanning Tree Protocol

По умолчанию

По умолчанию указанные в пределах IEEE 802.1 TLV не заданы.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для конфигурирования физических портов. Если включено анонсирование дополнительных TLV, они будут инкапсулированы в LLDPDU и отправлены на другие устройства.

Тип Protocol Identity TLV определяет, анонсировать ли соответствующий экземпляр Protocol Identity локальной системы на порту. Protocol Identity TLV позволяет устройствам анонсировать протоколы, которые важны для работы сети. Например, такие протоколы как Spanning Tree Protocol, Link Aggregation Control Protocol и другие протоколы, установленные vendor-ом, отвечают за поддержку топологии и подключения к сети. Если работают обе функции протокола и на порту включено анонсирование Protocol Identity, Protocol Identity TLV будет анонсирован.

PPVID TLV будет отправлен на VLAN только при условии, что сконфигурированный VLAN ID соответствует настройкам Protocol VLAN на данном интерфейсе, а данная VLAN существует. VLAN будет анонсирована в VLAN Name TLV только при условии, что интерфейс является портом-членом сконфигурированного VLAN ID.

Пример

В данном примере показано, как включить анонсирование Port VLAN ID TLV.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp dot1-tlv-select port-vlan
Switch(config-if)#
```

В данном примере показано, как включить анонсирование Port and Protocol VLAN ID TLV. Анонсированные VLAN: от VLAN 1 до VLAN 3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp dot1-tlv-select protocol-vlan 1-3
Switch(config-if)#
```

В данном примере показано, как включить анонсирование VLAN Name TLV. Анонсированные VLAN: от VLAN 1 до VLAN 3.

```
Switch# configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#lldp dot1-tlv-select vlan-name 1-3
Switch(config-if)#
```

В данном примере показано, как включить анонсирование LACP Protocol Identity TLV.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp dot1-tlv-select protocol-identify lacp
Switch(config-if)#
```

52-4 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 | max-frame-size]
no lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | max-frame-size]

Параметры

mac-phy-cfg	(Опционально) Укажите MAC/PHY Configuration/Status TLV, который необходимо отправить. MAC/PHY Configuration/Status TLV – это дополнительный TLV, который определяет (1) режим дуплекса и максимальную скорость передачи узла 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.
link-aggregation	(Опционально) Укажите Link Aggregation TLV, который необходимо отправить. Link Aggregation TLV содержит информацию о том, можно ли агрегировать группу, агрегируется ли группа в данный момент, а также информацию об агрегированном port channel ID. Если порт не агрегирован, значение port channel ID – 0.
max-frame-size	(Опционально) Укажите Maximum Frame Size TLV, который необходимо отправить. Maximum Frame Size TLV указывает максимальный размер фрейма для используемого MAC и PHY.

По умолчанию

По умолчанию указанный в пределах IEEE 802.3 TLV не указан.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для конфигурирования физических портов. Если при помощи данной команды включено анонсирование дополнительных TLV, указанных в пределах IEEE 802.3, они будут инкапсулированы в LLDPDU и отправлены на другие устройства.

Если не указаны дополнительные параметры, будут выбраны все поддерживаемые TLV, указанные в пределах IEEE 802.3, или выбор всех TLV, указанных в пределах IEEE 802, будет отменен.

Пример

В данном примере показано, как включить анонсирование MAC/PHY Configuration/Status TLV.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp dot3-tlv-select mac-phy-cfg
Switch(config-if)#
```

52-5 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

Уровень команды по умолчанию

Уровень 12

Использование команды

При обнаружении LLDP MED Capabilities TLV будет запущена процедура Fast Start. Используйте данную команду, чтобы настроить количество отправляемых пакетов Fast Start, которое соответствует количеству передач LLDP-сообщений за один полный интервал Fast Start.

Пример

В данном примере показано, как сконфигурировать количество отправляемых пакетов Fast Start.

```
Switch# configure terminal
Switch(config)# lldp fast-count 10
Switch(config)#
```

52-6 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данный параметр – это множитель для интервала передачи LLDPDU, с помощью которого будет вычислено значение TTL в LLDPDU. Время жизни определяется при помощи множителя удержания, умноженного на интервал TX. Если TTL для определенного анонса на соседнем коммутаторе истек, анонсированная информация будет удалена из MIB соседнего устройства.

Пример

В данном примере показано, как указать значение 3 для множителя удержания LLDP.

```
Switch# configure terminal
Switch(config)# lldp hold-multiplier 3
Switch(config)#
```

52-7 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для конфигурирования физических портов. Используйте данную команду, чтобы указать IPv4/IPv6-адрес, передаваемый в Management Address TLV на указанном порту. Если IP-адрес указан, но адрес не ассоциирован с одним из интерфейсов системы, адрес не будет отправлен.

Если при использовании команды **lldp management-address** не указан ни один адрес, коммутатор обнаружит по крайней мере один IPv4/IPv6-адрес в VLAN с самым низким VLAN ID. Если подходящих IPv4/IPv6-адресов нет, Management Address TLV анонсирован не будет. После того как администратор сконфигурировал адрес, оба адреса управления по умолчанию (IPv4 и IPv6) станут неактивны и не будут отправлены. IPv4/IPv6-адрес по умолчанию снова станет активен, если все сконфигурированные адреса будут удалены. Используйте данную команду несколько раз, чтобы создать несколько адресов управления IPv4/IPv6.

Используйте команду **no lldp management-address** без адреса управления, чтобы отключить адрес управления, анонсированный в LLDPDU. При отсутствии в списке действительного адреса управления, Management Address TLV отправлен не будет.

Пример

В данном примере показано, как настроить адрес управления IPv4 на интерфейсах Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch# configure terminal
Switch(config)# interface range ethernet 1/0/1-1/0/2
Switch(config-if-range)# lldp management-address 10.1.1.1
Switch(config-if-range)#
```

В данном примере показано, как настроить адрес управления IPv6 на интерфейсах Ethernet 1/0/3 и Ethernet 1/0/4.

```
Switch# configure terminal
Switch(config)# interface range ethernet 1/0/3-1/0/4
Switch(config-if-range)# lldp management-address FE80::250:A2FF:FEBF:A056
Switch(config-if-range)#
```

В данном примере показано, как удалить адрес управления 10.1.1.1 из интерфейсов Ethernet 1/0/1 и Ethernet 1/0/2. Если 10.1.1.1 является последним адресом управления, Management Address TLV отправлен не будет.

```
Switch# configure terminal
Switch(config)# interface range ethernet 1/0/1-1/0/2
Switch(config-if-range)# no lldp management-address 10.1.1.1
Switch(config-if-range)#
```

В данном примере показано, как удалить адрес управления FE80::250:A2FF:FEBF:A056 из интерфейса Ethernet 1/0/3.

```
Switch# configure terminal
Switch(config)# interface range ethernet 1/0/3-1/0/4
Switch(config-if-range)# no lldp management-address FE80::250:A2FF:FEBF:A056
Switch(config-if-range)#
```

В данном примере показано, как удалить все адреса управления из интерфейса Ethernet 1/0/5. В этом случае на Ethernet 1/0/5 Management Address TLV отправлен не будет.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/5
Switch(config-if)# no lldp management-address
Switch(config-if)#
```

52-8 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]
no lldp med-tlv-select [capabilities | inventory-management | network-policy]
```

Параметры

capabilities	(Опционально) Укажите, чтобы передать LLDP-MED Capabilities TLV.
inventory-management	(Опционально) Укажите, чтобы передать LLDP-MED Inventory Management TLV.
network-policy	(Опционально) Укажите, чтобы передать LLDP-MED Network Policy TLV.

По умолчанию

LLDP-MED TLV по умолчанию не выбран.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для конфигурирования физических портов. Команда применяется для включения/отключения передачи LLDP-MED TLV.

При отключении передачи Capabilities TLV будут также отключены LLDP-MED на физическом интерфейсе: LLDP-MED TLV не будут отправляться, даже если другие LLDP-MED TLV включены.

По умолчанию коммутатор отправляет LLDP-пакеты до тех пор, пока получает пакеты LLDP-MED от конечного устройства. Коммутатор отправляет пакеты LLDP-MED до тех пор, пока получает LLDP- пакеты.

Пример

В данном примере показано, как включить передачу LLDP-MED TLV и LLDP-MED Capabilities TLV.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp med-tlv-select capabilities
Switch(config-if)#
```

52-9 lldp receive

Данная команда используется для того, чтобы включить на физическом интерфейсе получение LLDP-сообщений. Используйте форму **no**, чтобы отключить получение LLDP-сообщений.

lldp receive
no lldp receive

Параметры

Нет

По умолчанию

По умолчанию функция LLDP включена на всех поддерживаемых интерфейсах.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для конфигурирования физических портов. Команда применяется для того, чтобы включить на интерфейсе получение LLDP-сообщений. Если LLDP не включен, коммутатор не будет получать LLDP-сообщения.

Пример

В данном примере показано, как включить на физическом интерфейсе получение LLDP-сообщений.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp receive
Switch(config-if)#
```

52-10 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

Уровень команды по умолчанию

Уровень 12

Использование команды

При перезапуске физического интерфейса LLDP будет выдержан заданный интервал времени между последней командой `disable` и повторной инициализацией.

Пример

В данном примере показано, как сконфигурировать интервал перед повторной инициализацией. Указанное значение – 5 секунд.

```
Switch# configure terminal
Switch(config)# lldp reinit 5
Switch(config)#
```

52-11 lldp run

Данная команда используется для глобального включения функции LLDP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

lldp run
no lldp run

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы глобально включить функцию LLDP и инициировать передачу, получение и обработку LLDP-пакетов на коммутаторе. Используйте команду **lldp transmit**, чтобы контролировать передачу LLDP-пакетов, и команду **lldp receive**, чтобы контролировать получение LLDP-пакетов. Обе команды применяются в режиме Interface Configuration Mode. Для корректной работы на физическом интерфейсе необходимо включить LLDP как на физическом интерфейсе, так и глобально.

При анонсировании LLDP-пакетов коммутатор передает информацию соседним устройствам через физические интерфейсы. Коммутатор изучает информацию об управлении и возможности подключения, содержащуюся в LLDP-пакетах, анонсированных соседними устройствами.

Пример

В данном примере показано, как включить функцию LLDP.

```
Switch# configure terminal
Switch(config)# lldp run
Switch(config)#
```

52-12 lldp forward

Данная команда используется для включения состояния LLDP Forwarding. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

lldp forward
no lldp forward

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная функция глобально контролирует передачу LLDP. Если состояние LLDP Global отключено, а функция LLDP Forwarding включена, полученный LLDPDU-пакет будет передан.

Пример

В данном примере показано, как включить состояние LLDP Forwarding глобально.

```
Switch# configure terminal
Switch(config)# lldp forward
Switch(config)#
```

52-13 lldp tlv-select

Данная команда используется для выбора TLV в наборе 802.1AB Basic Management, а также для передачи TLV и его инкапсулирования в LLDPDU с последующей отправкой на соседние устройства. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

lldp tlv-select [port-description | system-capabilities | system-description | system-name]
no lldp tlv-select [port-description | system-capabilities | system-description | system-name]

Параметры

port-description	(Опционально) Укажите Port Description TLV, который необходимо отправить. Port Description TLV позволяет анонсировать описание порта IEEE 802 LAN station.
system-capabilities	(Опционально) Укажите System Capabilities TLV, который необходимо отправить. Поле System Capabilities будет содержать bit-map, определяющий основные функции системы.
system-description	(Опционально) Укажите System Description TLV, который необходимо отправить. System Description должно включать полное имя и версию аппаратного обеспечения, операционной системы и программного обеспечения.
system-name	(Опционально) Укажите System Name TLV, который необходимо отправить. System Name должно представлять собой полное имя домена системы.

По умолчанию

По умолчанию дополнительный 802.1AB Basic Management TLV не указан.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для конфигурирования физических портов. Команда применяется для выбора дополнительных TLV, которые необходимо передать. Если выбрано анонсирование дополнительных TLV, они будут инкапсулированы в LLDPDU и отправлены на другие устройства.

Пример

В данном примере показано, как включить все поддерживаемые дополнительные 802.1AB Basic Management TLV.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp tlv-select
Switch(config-if)#
```

В данном примере показано, как включить анонсирование System Name TLV.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp tlv-select system-name
Switch(config-if)#
```

52-14 lldp transmit

Данная команда используется для включения анонсирования/передачи LLDP. Используйте форму **no**, чтобы отключить передачу LLDP.

lldp transmit
no lldp transmit

Параметры

Нет

По умолчанию

По умолчанию передача LLDP включена на всех поддерживаемых интерфейсах.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для конфигурирования физических портов. Команда применяется для включения передачи LLDP на физическом интерфейсе. Если LLDP не функционирует, коммутатор не будет передавать LLDP-сообщения.

Пример

В данном примере показано, как включить передачу LLDP.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp transmit
Switch(config-if)#
```

52-15 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Значение LLDP Transmission Interval должно быть больше или равно значению таймера Transmission Delay, умноженному на четыре.

Пример

В данном примере показано, как указать значение таймера Transmission Delay. Заданное значение – 8 секунд.

```
Switch# configure terminal
Switch(config)# lldp tx-delay 8
Switch(config)#
```

52-16 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данный интервал определяет скорость передачи LLDP-пакетов.

Пример

В данном примере показано, как сконфигурировать отправку обновлений LLDP через каждые 50 секунд.

```
Switch# configure terminal
Switch(config)# lldp tx-interval 50
Switch(config)#
```

52-17 snmp-server enable traps lldp

Данная команда используется для включения отправки LLDP Trap и LLDP-MED Trap. Используйте форму **no**, чтобы отключить данную функцию.

```
snmp-server enable traps lldp [med]
no snmp-server enable traps lldp [med]
```

Параметры

med	(Опционально) Укажите, чтобы включить отправку LLDP-MED Trap.
------------	---

По умолчанию

По умолчанию отправка LLDP Trap и LLDP-MED Trap отключены.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду **snmp-server enable traps lldp**, чтобы включить отправку LLDP-уведомлений.

Используйте команду **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)#
```

52-18 lldp notification enable

Данная команда используется для включения отправки уведомлений LLDP и LLDP-MED на интерфейсе. Используйте форму **no**, чтобы отключить данную функцию.

lldp [med] notification enable
no lldp [med] notification enable

Параметры

med	(Опционально) Укажите, чтобы включить уведомления LLDP-MED.
------------	---

По умолчанию

По умолчанию уведомления LLDP и LLDP-MED отключены.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду **lldp notification enable**, чтобы включить отправку уведомлений LLDP.

Используйте команду **lldp med notification enable**, чтобы включить отправку уведомлений LLDP-MED.

Пример

В данном примере показано, как включить отправку уведомлений LLDP-MED для интерфейса Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp med notification enable
Switch(config-if)#
```

52-19 lldp subtype

Данная команда используется для настройки подтипа LLDP TLV.

lldp subtype port-id {mac-address | local}

Параметры

port-id	Укажите подтип Port ID TLV.
mac-address	Укажите, чтобы обозначить подтип Port ID TLV как «MAC Address (3)», а также чтобы закодировать MAC-адрес в поле «port ID».
local	Укажите, чтобы обозначить подтип Port ID TLV как «Locally assigned (7)», а также чтобы закодировать номер порта в поле «port ID».

По умолчанию

Подтип Port ID TLV по умолчанию – local (port number).

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать подтип LLDP TLV. Подтип Port ID указывает, как обозначен порт в поле port ID.

Пример

В данном примере показано, как сконфигурировать подтип Port ID TLV. Указанный подтип – mac- address.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp subtype port-id mac-address
Switch(config-if)#
```

52-20 show lldp

Данная команда используется для отображения общих настроек функции LLDP на коммутаторе.

show lldp

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить общие настройки функции LLDP на коммутаторе.

Пример

В данном примере показано, как отобразить общие настройки функции LLDP на коммутаторе.

```

Switch#show lldp

LLDP System Information
  Chassis ID Subtype      : MAC Address
  Chassis ID              : F0-7D-68-36-30-B0
  System Name             : Switch
  System Description      : Gigabit Ethernet Switch
  System Capabilities Supported: Repeater, Bridge
  System Capabilities Enabled : Repeater, Bridge
LLDP-MED System Information:
  Device Class           : Network Connectivity Device
  Hardware Revision      : A1
  Firmware Revision      : 1.00.001
  Software Revision      : 1.00.001
  Serial Number          : DGS3130111013
  Manufacturer Name      : D-Link Corporation
  Model Name             : DGS-3130-30TS Gigabit Ethernet S
  Asset ID               :

LLDP Configurations
  LLDP State             : Disabled
  LLDP Forward State     : Disabled
  Message TX Interval    : 30
  Message TX Hold Multiplier: 4
  ReInit Delay           : 2
  TX Delay               : 2

LLDP-MED Configuration:
  Fast Start Repeat Count : 4

Switch#

```

52-21 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

User/Privileged EXEC Mode Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию о функции LLDP для каждого физического интерфейса.

Пример

В данном примере показано, как отобразить настройки функции LLDP для указанного физического интерфейса.

```

Switch#show lldp interface ethernet 1/0/1

Port ID: 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                       :Disabled
    (None)
  Enabled Protocol_Identity
    (None)
IEEE 802.3 Organizationally Specific TLVs:
  MAC/PHY Configuration/Status           :Disabled
  Link Aggregation                        :Disabled
  Maximum Frame Size                      :Disabled
  Energy Efficient Ethernet               :Disabled
LLDP-MED Organizationally Specific TLVs:
  LLDP-MED Capabilities TLV               :Disabled
  LLDP-MED Network Policy TLV            :Disabled
  LLDP-MED Inventory TLV                 :Disabled
LLDP-DCBX Organizationally Specific TLVs:
  LLDP-DCBX ETS Configuration TLV        :Disabled
  LLDP-DCBX ETS Recommendation TLV       :Disabled
  LLDP-DCBX Priority-based Flow Control Configuration TLV :Disabled

Switch#

```

Отображаемые параметры

Enabled Management Address

Отображает включенные IPv4/IPv6-адреса. «(None)» означает, что пользователь не сконфигурировал адрес управления (Management Address) при помощи команды **lldp management-address** или включенные IPv4/IPv6-адреса по умолчанию не применяются.

Enabled Port and Protocol VLAN ID	Отображает включенные Port and Protocol VLAN. В список VLAN включены сконфигурированные и включенные VLAN. При отсутствии сконфигурированных PPVID VLAN отображается «(None)».
Enabled VLAN Name	Отображает включенные VLAN для отправки VLAN Name TLV. В список VLAN включены сконфигурированные и включенные VLAN. При отсутствии сконфигурированных VLAN для VLAN Name TLV отображается «(None)».
Enabled Protocol Identity	Отображает включенную строку протокола для Protocol Identity TLV. При отсутствии включенных протоколов для Protocol Identity TLV отображается «(None)».

52-22 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.
brief	(Опционально) Укажите, чтобы отобразить информацию в сокращенном формате.
detail	(Опционально) Укажите, чтобы отобразить информацию в подробном формате. Если не указан ни параметр brief , ни параметр detail , информация будет отображена в стандартном формате.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить текущую анонсируемую локальную информацию в исходящих LLDP-объявлениях для каждого физического интерфейса.

Пример

В данном примере показано, как отобразить локальную информацию для интерфейса физического порта Ethernet 1/0/1 в подробном формате.

```
Switch#show lldp local interface ethernet 1/0/1 detail

Port ID: eth1/0/1
-----
Port ID Subtype           : Local
Port ID                   : eth1/0/1
Port Description          : D-Link Corporation DGS-3130-30TS HW
                          A1 firmware 1.00.001 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                : 1.3.6.1.4.1.171.10.147.1.1

  Address 2 :
    Subtype           : IPv4
    Address            : 10.90.90.90
    IF Type            : IfIndex
    OID                : 1.3.6.1.4.1.171.10.147.1.1

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-3130-30TS HW
                          A1 firmware 1.00.001 Port 1 on Unit
                          1
Port PVID                  : 1
Management Address Count  : 2
PPVID Entries Count       : 0
VLAN Name Entries Count   : 1
Protocol Identity Entries Count : 0
MAC/PHY Configuration/Status : (See Detail)
Link Aggregation          : (See Detail)
Maximum Frame Size        : 1536
Energy Efficient Ethernet : (See Detail)
LLDP-MED capabilities     : (See Detail)
Network Policy            : (See Detail)
LLDP-DCBX capabilities    : (See Detail)

Switch#

```

В данном примере показано, как отобразить локальную информацию для интерфейса физического порта Ethernet 1/0/1 в сокращенном формате.

```

Switch#show lldp local interface ethernet 1/0/1 brief

Port ID: eth1/0/1
-----
Port ID Subtype           : Local
Port ID                   : eth1/0/1
Port Description          : D-Link Corporation DGS-3130-30TS HW
                          A1 firmware 1.00.001 Port 1 on Unit
                          1

Switch#

```

52-23 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

User/Privileged EXEC Mode Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию об адресе управления.

Пример

В данном примере показано, как отобразить всю информацию об адресе управления.

```
Switch# show lldp management-address

Address 1 : (default)
-----
Subtype           : IPv4
Address           : 10.90.90.90
IF Type          : IfIndex
OID              : 1.3.6.1.4.1.171.10.118.2
Advertising Ports : -

Address 2 :
-----
Subtype           : IPv4
Address           : 10.90.90.90
IF Type          : IfIndex
OID              : 1.3.6.1.4.1.171.10.118.2
Advertising Ports : -

Total Entries : 2

Switch#
```

52-24 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.
brief	(Опционально) Укажите, чтобы отобразить информацию в сокращенном формате.
detail	(Опционально) Укажите, чтобы отобразить информацию в подробном формате. Если не указан ни параметр brief , ни параметр detail , информация будет отображена в стандартном формате.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию, полученную от соседних устройств.

Пример

В данном примере показано, как отобразить информацию о соседних устройствах, изученную LLDP на интерфейсе eth1/0/9, в подробном формате.

```

Switch# show lldp neighbor interface eth1/0/9 detail

Port ID : eth1/0/9
-----
Remote Entities Count : 1
Entity 1
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-01-02-03-04-05
  Port ID Subtype        : Local
  Port ID                 : eth1/0/5
  Port Description       : RMON Port
  System Name            : Switch1
  System Description     : Stackable Ethernet Switch
  System Capabilities Supported : Repeater, Bridge
  System Capabilities Enabled   : Repeater, Bridge
  Management Address Count : 0
  (None)
  Port VLAN ID           : 0
  PPVID Entries Count    : 0
  (None)
  VLAN Name Entries Count : 0
  (None)
  Protocol ID Entries Count : 0
  (None)
  MAC/PHY Configuration/Status : (None)
  Power Via MDI          : (None)
  Link Aggregation       : (None)
  Maximum Frame Size     : 0
  Unknown TLVs Count     : 0
  (None)
LLDP-MED capabilities      :
LLDP-MED device class     : Endpoint device class III
  LLDP-MED capabilities support :
    LLDP-MED capabilities      : Support
    Network Policy             : Support
    Location identification     : Not Support
    Extended power via MDI     : Support
    Inventory                   : Support
  LLDP-MED capabilities enabled :
    LLDP-MED capabilities      : Enabled
    Network Policy             : Enabled
    Location identification     : Enabled
    Extended power via MDI     : Enabled
    Inventory                   : Enabled
  Extended power via MDI      :
    Power device type          : PD device
    Power Source                : from PSE
    Power request               : 8 watts
Network policy              :
  Application type            : Voice
  VLAN ID                     : -
  Priority                     : -
  DSCP                        : -
  Unknown                     : True
  Tagged                       : -
  Inventory Management        :
  (None)

Switch#

```

В данном примере показано, как отобразить информацию о Remote LLDP в стандартном формате.

```
Switch# show lldp neighbor interface ethernet 1/0/1

Port ID : 1
-----
Remote Entities Count : 2
Entity 1
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-01-02-03-04-01
  Port ID Subtype        : Local
  Port ID                 : eth1/0/1
  Port Description       : RMON Port 1 on Unit 1
  System Name            : Switch1
  System Description     : Stackable Ethernet Switch
  System Capabilities Supported : Repeater, Bridge
  System Capabilities Enabled  : Repeater, Bridge
  Management Address Count   : 1
  Port VLAN ID              : 1
  PPVID Entries Count       : 5
  VLAN Name Entries Count   : 3
  Protocol ID Entries Count : 2
  MAC/PHY Configuration Status : (See Detail)
  Power Via MDI             : (See Detail)
  Link Aggregation         : (See Detail)
  Maximum Frame Size       : 1536
  LLDP-MED capabilities    : (See Detail)
  Network policy           : (See Detail)
  Extended Power Via MDI   : (See Detail)
  Inventory Management     : (See Detail)
  Unknown TLVs Count       : 2
Entity 2
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-01-02-03-04-02
  Port ID Subtype        : Local
  Port ID                 : eth1/0/1
  Port Description       : RMON Port 1 on Unit 2
  System Name            : Switch2
  System Description     : Stackable Ethernet Switch
  System Capabilities Supported : Repeater, Bridge
  System Capabilities Enabled  : Repeater, Bridge
  Management Address Count   : 2
  Port VLAN ID              : 1
  PPVID Entries Count       : 5
  VLAN Name Entries Count   : 3
  Protocol Id Entries Count : 2
  MAC/PHY Configuration Status : (See Detail)
  Power Via MDI             : (See Detail)
  Link Aggregation         : (See Detail)
  Maximum Frame Size       : 1536
  LLDP-MED capabilities    : (See Detail)
  Extended power via MDI   : (See Detail)
  Network policy           : (See Detail)
  Inventory Management     : (See Detail)
  Unknown TLVs Count       : 2
Switch#
```

В данном примере показано, как отобразить информацию о соседних устройствах на интерфейсах от Ethernet 1/0/1 до Ethernet 1/0/2 в кратком формате.

```

Switch# show lldp neighbor interface ethernet 1/0/1-1/0/2 brief

Port ID: eth1/0/1
-----
Remote Entities Count : 2
Entity 1
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-01-02-03-04-01
  Port ID Subtype        : Local
  Port ID                 : eth1/0/1
  Port Description       : RMON Port 1 on Unit 3
Entity 2
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-01-02-03-04-02
  Port ID Subtype        : Local
  Port ID                 : eth1/0/2
  Port Description       : RMON Port 1 on Unit 4

Port ID : eth1/0/2
-----
Remote Entities Count : 3
Entity 1
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-01-02-03-04-03
  Port ID Subtype        : Local
  Port ID                 : eth1/0/4
  Port Description       : RMON Port 2 on Unit 1
Entity 2
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-01-02-03-04-04
  Port ID Subtype        : Local
  Port ID                 : eth1/0/5
  Port Description       : RMON Port 2 on Unit 2
Entity 3
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-01-02-03-04-05
  Port ID Subtype        : Local
  Port ID                 : eth1/0/6
  Port Description       : RMON Port 2 on Unit 3

Total Entries: 2

Switch#

```

52-25 show lldp traffic

Данная команда используется для отображения глобальной информации о трафике LLDP.

show lldp traffic

Параметры

Нет

По умолчанию

Нет

Режим ввода командыUser/Privileged EXEC Mode
Любой режим конфигурирования**Уровень команды по умолчанию**

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию об обнаружении соседних устройств на коммутаторе.

Пример

В данном примере показано, как отобразить глобальную информацию о трафике LLDP.

```
Switch#show lldp traffic

Last Change Time   : 7958183
Total Inserts      : 7
Total Deletes      : 0
Total Drops        : 0
Total Ageouts      : 0

Switch#
```

Отображаемые параметры

Last Change Time	Время после последнего обновления до удаленной таблицы в днях, часах, минутах и секундах.
Total Inserts	Общее количество вставок в удаленную таблицу.
Total Deletes	Общее количество удалений из удаленной таблицы.
Total Drops	Общее количество случаев получения данных, которые не были добавлены в таблицу из-за непригодности.
Total Ageouts	Общее количество случаев удаления записей после истечения интервала Time to Live.

52-26 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

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить трафик LLDP на каждом физическом интерфейсе.

Пример

В данном примере показано, как отобразить статистику для порта 1.

```
Switch#show lldp traffic interface ethernet 1/0/1

Port ID : eth1/0/1
-----
Total Transmits      : 0
Total Discards       : 0
Total Errors         : 0
Total Receives       : 0
Total TLV Discards   : 0
Total TLV Unknowns   : 0
Total Ageouts        : 0

Switch#
```

Отображаемые параметры

Total Transmits	Общее количество LLDP-пакетов, переданных на порту.
Total Discards	Общее количество LLDP-кадров, отброшенных на порту.
Total Errors	Количество недействительных LLDP-кадров, полученных на порту.
Total Receives	Общее количество LLDP-пакетов, полученных на порту.

Total TLV Discards	Количество отброшенных TLV.
Total TLV Unknowns	Общее количество полученных на порту LLDP TLV, тип которых находится в зарезервированном диапазоне и не распознается.
Total Ageouts	Общее количество случаев удаления записей на порту после истечения интервала Time to Live.

53. Команды Loopback Detection (LBD)

53-1 loopback-detection (Global)

Данная команда используется для того, чтобы включить функцию LBD (Loopback Detection) глобально. Используйте форму **no**, чтобы глобально отключить данную функцию.

```
loopback-detection [mode {port-based | vlan-based}]
no loopback-detection [mode]
```

Параметры

mode	(Опционально) Укажите режим обнаружения.
port-based	Укажите режим обнаружения петли port-based (на порту).
vlan-based	Укажите режим обнаружения петли VLAN-based (в VLAN).

По умолчанию

По умолчанию данная опция отключена.
Режим обнаружения по умолчанию – port-based.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Обычно режим port-based используется на портах, к которым подключены пользователи, а режим VLAN-based используется на trunk-портах и гибридных портах, если соседнее устройство не поддерживает функцию LBD.

Если включен режим port-based, порт, на котором включена функция LBD, будет отправлять нетегированные пакеты port-based LBD, чтобы обнаружить петлю. При наличии на пути петли передаваемый пакет вернется на тот же порт или на другой порт того же устройства. При обнаружении портом, на котором включена функция LBD, петли, на порту будет отключена передача и получение пакетов.

Если включен режим VLAN-based, порт будет периодически отправлять пакеты VLAN-based LBD на каждую VLAN, членом которой является данный порт, и на которой включена функция LBD. Если порт является тегированным членом VLAN, будут отправлены тегированные пакеты LBD. Если порт является нетегированным членом VLAN, будут отправлены нетегированные пакеты LBD. При наличии на пути VLAN петли, передача и получение пакетов будет временно остановлена на том порту закольцованной VLAN, где была обнаружена петля.

Если порт, на котором отключена функция LBD, получает пакет LBD и обнаруживает, что пакет отправлен системой, возможны два варианта: если тип данного пакета – port-based LBD, будет заблокирован порт отправления, а если тип пакета – VLAN-based LBD, будет заблокирована VLAN порта отправления.

Если на порту сконфигурирован режим VLAN-based, а порт является нетегированным членом нескольких VLAN, будет отправлен один нетегированный пакет LBD на каждую VLAN с указанием номера VLAN в поле VLAN пакета.

Восстановить порт, отключенный из-за ошибки, можно двумя способами: используйте команду **errdisable recovery cause loopback-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)#
```

53-2 loopback-detection (Interface)

Данная команда используется для включения функции LBD на интерфейсе. Используйте форму **no**, чтобы отключить данную функцию на интерфейсе.

loopback-detection
no loopback-detection

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить функцию LBD на интерфейсе. Команда применяется для конфигурирования физических портов и port-channel.

Пример

В данном примере показано, как включить функцию LBD на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# loopback-detection
Switch(config-if)#
```

53-3 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

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы сконфигурировать интервал передачи пакетов LBD, отправляемых для обнаружения петли.

Пример

В данном примере показано, как сконфигурировать интервал 20 секунд.

```
Switch# configure terminal
Switch(config)# loopback-detection interval 20
Switch(config)#
```

53-4 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

VLAN-LIST

Укажите идентификационный номер / номера / диапазон номеров VLAN. Чтобы указать список диапазонов VLAN, введите одно или несколько значений, разделяя их при помощи запятых или дефисов.

По умолчанию

По умолчанию данная опция включена для всех VLAN.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команд

Используйте данную команду, чтобы сконфигурировать список VLAN, на которых включена функция LBD. Настройки команды будут применены, если на порту сконфигурирован режим обнаружения петли VLAN-based.

По умолчанию пакеты LBD Control отправляются на все VLAN, членом которых является данный порт. Пакеты LBD Control отправляются на VLAN, членом которых является данный порт из указанного списка VLAN.

Список VLAN можно расширить, применив команду несколько раз.

Пример

В данном примере показано, как включить функцию LBD в диапазоне с VLAN 100 по VLAN 200.

```
Switch# configure terminal
Switch(config)# loopback-detection vlan 100-200
Switch(config)#
```

53-5 show loopback-detection

Данная команда используется для отображения текущих настроек LBD.

show loopback-detection [interface INTERFACE-ID [, | -]]

Параметры

interface INTERFACE-ID	(Опционально) Укажите интерфейс, который необходимо отобразить.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить настройки и статус функции LBD.

Пример

В данном примере показано, как отобразить текущие настройки и статус функции LBD.

```
Switch#sh loopback-detection
```

```
Loop Detection      : Enabled
Detection Mode      : port-based
LBD enabled VLAN    : all VLANs
Interval            : 20 seconds
Action Mode         : Shutdown
Address Type        : Multicast
Function Version     : v4.07
```

Interface	State	Result	Time Left (sec)
eth1/0/1	Enabled	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 ethernet 1/0/1

Interface      State      Result      Time Left (sec)
-----      -
eth1/0/1      Enabled    Normal      -

Switch#
```

Отображаемые параметры

Interface	Отображает порт, на котором включена функция LBD.
State	Отображает статус порта.
Result	Отображает, обнаружена ли петля.
Time Left	Отображает время, оставшееся до автовосстановления.

53-6 loopback-detection action

Данная команда используется для настройки режима LBD. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
loopback-detection action {shutdown | none}
no loopback-detection action
```

Параметры

shutdown	Укажите, чтобы отключить порт в режиме port-based / заблокировать трафик на указанной VLAN в режиме VLAN-based при обнаружении петли.
none	Укажите, чтобы не отключать порт в режиме port-based / не блокировать трафик на указанной VLAN в режиме VLAN-based при обнаружении петли.

По умолчанию

Параметр по умолчанию – **shutdown**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить режим LBD.

Пример

В данном примере показано, как настроить режим LBD.

```
Switch# configure terminal
Switch(config)# loopback-detection action none
Switch(config)#
```

53-7 snmp-server enable traps loopback-detection

Данная команда используется для включения отправки SNMP-уведомлений для LBD. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
snmp-server enable traps loopback-detection
no snmp-server enable traps loopback-detection
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить отработку SNMP-уведомлений для LBD. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

Пример

В данном примере показано, как включить отработку SNMP-уведомлений для LBD.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps loopback-detection
Switch(config)#
```

53-8 loopback-detection address-type

Данная команда используется для того, чтобы настроить тип адреса назначения (destination) пакетов LBD. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
loopback-detection address-type {multicast | broadcast}
no loopback-detection address-type
```

Параметры

multicast	Укажите, чтобы отсылать только групповые пакеты LBD. Адрес назначения – CF-00-00-00-00-00.
broadcast	Укажите, чтобы отсылать только ширококвещательные пакеты LBD. Адрес назначения – FF-FF-FF-FF-FF-FF.

По умолчанию

Параметр по умолчанию – **multicast**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить тип адреса назначения пакетов LBD.

Пример

В данном примере показано, как настроить тип адреса назначения пакетов LBD. Указанный тип – broadcast.

```
Switch#configure terminal
Switch(config)#loopback-detection address-type broadcast
Switch(config)#
```


54. Команды аутентификации MAC

54-1 mac-auth system-auth-control

Данная команда используется для глобального включения MAC-аутентификации. При использовании формы **no** команда отключит глобальную MAC-аутентификацию.

```
mac-auth system-auth-control
no mac-auth system-auth-control
```

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

MAC-аутентификация – это функция, предназначенная для аутентификации пользователя на основе MAC-адреса при попытке доступа к сети через коммутатор. Сам коммутатор может выполнять аутентификацию на основе локальной базы данных или выполнять процесс аутентификации для клиентов на удаленном сервере с использованием протокола RADIUS.

Пример

В данном примере показано, как включить MAC-аутентификацию глобально.

```
Switch# configure terminal
Switch(config)# mac-auth system-auth-control
Switch(config)#
```

54-2 mac-auth enable

Данная команда используется для включения MAC-аутентификации на указанном интерфейсе. При использовании формы **no** команда отключит MAC-аутентификацию.

```
mac-auth enable
no mac-auth enable
```

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда доступна только для настройки интерфейса физического порта. Она может использоваться для включения MAC-аутентификации на указанном интерфейсе.

Также MAC-аутентификация имеет следующие ограничения:

- MAC-аутентификация на порту не может быть включена, если на данном порту включена функция Port Security.
- MAC-аутентификация на порту не может быть включена, если на данном порту включена функция IP-MAC-Port-Binding.
- MAC-аутентификация на порту не может быть включена на порту, где настроено агрегирование каналов.

Пример

В данном примере показано, как включить MAC-аутентификацию на Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# mac-auth enable
Switch(config-if)#
```

54-3 mac-auth password

Данная команда используется для настройки пароля аутентификации для локальной и RADIUS-аутентификации. При использовании формы **no** команда вернется к значениям по умолчанию.

mac-auth password [0 | 7] STRING
no mac-auth password

Параметры

0	(Опционально) Пароль в обычном текстовом виде. Если не указан ни 0, ни 7, по умолчанию пароль будет в обычном текстовом виде.
7	(Опционально) Зашифрованный пароль. Если не указан ни 0, ни 7, по умолчанию пароль будет в обычном текстовом виде.
password STRING	Укажите, чтобы задать пароль для MAC-аутентификации. Если указан пароль в обычном текстовом виде, длина

строки не может превышать 16 символов.

По умолчанию

По умолчанию паролем является MAC-адрес клиента.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для настройки пароля, используемого для аутентификации пользователей по MAC-адресу. Если команда не настроена, пароль для аутентификации пользователя по MAC-адресу будет сформирован на основе MAC-адреса. Формат MAC-адреса может быть настроен с помощью команды **authentication mac username format**.

Пример

В данном примере показано, как настроить пароль MAC-аутентификации.

```
Switch# configure terminal
Switch(config)# mac-auth password newpass
Switch(config)#
```

54-4 mac-auth username

Данная команда используется для настройки имени пользователя для локальной и RADIUS-аутентификации. При использовании формы **no** команда вернется к значениям по умолчанию.

mac-auth username *STRING*
no mac-auth username

Параметры

<i>STRING</i>	Укажите, чтобы задать имя пользователя для MAC-аутентификации. Длина строки не может превышать 16 символов.
---------------	---

По умолчанию

По умолчанию именем пользователя является MAC-адрес клиента.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для настройки имени пользователя для аутентификации пользователей по MAC-адресу. Это имя пользователя используется для аутентификации через локальную базу данных и удаленные серверы. Если команда не настроена, имя пользователя для аутентификации будет формироваться на основе MAC-адреса.

Пример

В данном примере показано, как настроить имя пользователя для MAC-аутентификации.

```
Switch# configure terminal
Switch(config)# mac-auth username user1
Switch(config)#
```

54-5 snmp-server enable traps mac-auth

Данная команда используется для включения отправки SNMP-уведомлений для MAC-аутентификации. При использовании формы **no** команда отключит SNMP-уведомления.

```
snmp-server enable traps mac-auth
no snmp-server enable traps mac-auth
```

Параметры

Нет

По умолчанию

По умолчанию функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Нет

Пример

В данном примере показано, как включить отработку трапов для MAC-аутентификации.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps mac-auth
Switch(config)#
```

55. Команды Mirror

55-1 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*

Параметры

<i>SESSION-NUMBER</i>	Укажите номер сессии мониторинга. Доступный диапазон значений: от 1 до 4.
<i>INTERFACE-ID</i>	Укажите интерфейс назначения для сессии мониторинга.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить интерфейс назначения для локальной сессии мониторинга или интерфейс назначения на коммутаторе назначения для сессии RSPAN.

В качестве интерфейсов назначения для сессий мониторинга можно использовать физические порты и port-channel. Для сессии мониторинга можно указать несколько интерфейсов источника, но только один интерфейс назначения. Интерфейс не может быть одновременно интерфейсом источника одной сессии и портом назначения другой сессии. Интерфейс можно сконфигурировать в качестве интерфейса назначения нескольких сессий, но в качестве интерфейса источника только одной сессии.

Используйте команду **monitor session source remote vlan** на коммутаторе назначения сессии RSPAN, чтобы сконфигурировать VLAN, на которую туннелируются отслеживаемые пакеты источника с удаленного сайта.

Пример

В данном примере показано, как создать сессию мониторинга порта с номером 1, указав физический порт Ethernet 1/0/1 в качестве порта назначения, а три физических порта источника (от Ethernet 1/0/2 до Ethernet 1/0/4) в качестве портов источника.

```
Switch# configure terminal
Switch(config)# monitor session 1 destination interface ethernet 1/0/1
Switch(config)# monitor session 1 source interface ethernet 1/0/2-4
Switch(config)#
```

55-2 monitor session destination remote vlan

Данная команда используется для настройки RSPAN VLAN и порта назначения (destination) для сессии источника (source) RSPAN. Используйте форму **no**, чтобы удалить настройки RSPAN VLAN.

monitor session *SESSION-NUMBER* **destination remote vlan** *VLAN-ID* **interface** *INTERFACE-ID*
monitor session *SESSION-NUMBER* **destination remote vlan access-list** *ACCESS-LIST-NAME* **replace**
vlan *VLAN-ID*
no monitor session *SESSION-NUMBER* **destination remote vlan** [**access-list** *ACCESS-LIST-NAME*]

Параметры

<i>SESSION-NUMBER</i>	Укажите номер сессии мониторинга. Доступный диапазон значений: от 1 до 4.
<i>VLAN-ID</i>	Укажите RSPAN VLAN, используемую для туннелирования отслеживаемых пакетов на удаленный сайт. Доступный диапазон значений: от 2 до 4094.
interface <i>INTERFACE-ID</i>	Укажите интерфейс, с помощью которого необходимо передать отслеживаемые пакеты на удаленный сайт.
access-list <i>ACCESS-LIST-NAME</i>	(Опционально) Укажите поток, используемый для замены RSPAN VLAN потока. Поток будет сконфигурирован, даже если список доступа не существует.
replace vlan <i>VLAN-ID</i>	(Опционально) Укажите VLAN ID, используемый для замены RSPAN VLAN ID на соответствующий поток пакетов, передаваемых из порта назначения на коммутаторе источника RSPAN. Доступный диапазон значений: от 1 до 4094.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду на коммутаторе источника сессии RSPAN.

Используйте команду **monitor session destination remote vlan**, чтобы сконфигурировать порт назначения, используемый для передачи отслеживаемых пакетов, и RSPAN VLAN, используемую для тегирования отслеживаемых пакетов до удаленного сайта. Для одной сессии можно сконфигурировать только один

интерфейс назначения. Порт назначения не может являться портом-членом RSPAN VLAN. В качестве порта назначения можно использовать физический порт или port-channel.

Каждую сессию необходимо сконфигурировать с уникальной RSPAN VLAN. При помощи данной команды нельзя указать интерфейс, с которого будут переданы отслеживаемые пакеты для нескольких сессий RSPAN.

Укажите список доступа для пакетов, отслеживаемых сессией, чтобы определить поток. RSPAN VLAN ID, использующийся для туннелирования данных пакетов, будет заменен на Replace VLAN ID. Для сессии источника RSPAN можно сконфигурировать несколько потоков замещения VLAN. RSPAN VLAN в удаленных сессиях используется только для отслеживания трафика.

Используйте команду **monitor session source interface**, чтобы сконфигурировать порты источника, пакеты которых будут отслеживаться.

Используйте команду **remote-span** в режиме VLAN Configuration Mode, чтобы указать VLAN в качестве RSPAN VLAN. Отслеживаемые пакеты будут туннелированы через trunk-порты-участники RSPAN VLAN следующих устройств.

Пример

В данном примере показано, как создать сессию RSPAN на коммутаторе источника. VLAN 100 указана в качестве RSPAN VLAN, порт назначения Ethernet 1/0/6 и три порта источника (Ethernet 1/0/2, Ethernet 1/0/3 и Ethernet 1/0/4) указаны в качестве отслеживаемых портов.

```
Switch# configure terminal
Switch(config)# monitor session 2 source interface ethernet 1/0/2-4
Switch(config)# monitor session 2 destination remote vlan 100 interface ethernet 1/0/6
Switch(config)#
```

55-3 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**] | **cpu rx**}
no monitor session *SESSION-NUMBER* **source interface** {*INTERFACE-ID* [, | -] | **cpu rx**}

Параметры

<i>SESSION-NUMBER</i>	Укажите номер сессии мониторинга. Доступный диапазон значений: от 1 до 4.
interface <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.
both	(Опционально) Укажите, чтобы отслеживать пакеты, переданные и полученные портом.
rx	(Опционально) Укажите, чтобы отслеживать пакеты, полученные портом.

tx	(Опционально) Укажите, чтобы отслеживать пакеты, переданные портом.
cpu rx	Укажите зеркалирование пакетов, полученных ЦПУ. Все пакеты, полученные ЦПУ, будут зеркалированы.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

В качестве интерфейсов источника для сессий мониторинга можно использовать физические порты и port-channel.

Для сессии мониторинга можно указать несколько интерфейсов источника, но только один интерфейс назначения (destination). Интерфейс не может быть одновременно интерфейсом источника одной сессии и портом назначения другой сессии. Интерфейс можно сконфигурировать в качестве интерфейса назначения нескольких сессий, но в качестве интерфейса источника только одной сессии.

Если направление не указано или указан параметр **both**, отслеживается как переданный, так и полученный трафик.

Пример

В данном примере показано, как создать сессию мониторинга порта с номером 1. Физический порт Ethernet 1/0/1 указан в качестве порта назначения, а три физических порта источника (от Ethernet 1/0/2 до Ethernet 1/0/4) указаны в качестве портов источника.

```
Switch# configure terminal
Switch(config)# monitor session 1 destination interface ethernet 1/0/1
Switch(config)# monitor session 1 source interface ethernet 1/0/2-4
Switch(config)#
```

55-4 monitor session source acl

Данная команда используется для того, чтобы сконфигурировать список доступа для мониторинга на основе потока. Используйте форму **no**, чтобы удалить список доступа для мониторинга на основе потока.

monitor session *SESSION-NUMBER* **source acl** *ACCESS-LIST-NAME*
no monitor session *SESSION-NUMBER* **source acl** *ACCESS-LIST-NAME*

Параметры

<i>SESSION-NUMBER</i>	Укажите номер сессии мониторинга. Доступный диапазон значений: от 1 до 4.
-----------------------	---

<i>ACCESS-LIST-NAME</i>	Укажите зеркалирование на основе потока. Поддерживается только входное зеркалирование, могут отслеживаться только списки доступа адресов MAC, IP или IPv6. Зеркалирование на основе потока можно сконфигурировать, даже если список доступа не существует.
-------------------------	--

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команд

Можно отследить только один список доступа за одну сессию (один список доступа может включать несколько потоков). Используйте команды **access-group** или **vlan map**, чтобы отследить пакет, отфильтрованный при помощи списка доступа, применяемого для аппаратного оборудования.

Пример

В данном примере показано, как создать сессию мониторинга с номером 2. Список доступа MAC «MAC-Monitored-flow» указан в качестве источника мониторинга.

```
Switch# configure terminal
Switch(config)# monitor session 2 destination interface ethernet 1/0/1
Switch(config)# monitor session 2 source acl MAC-Monitored-flow
Switch(config)#
```

55-5 monitor session source remote vlan

Данная команда используется для того, чтобы настроить RSPAN VLAN для сессии назначения (destination) RSPAN. Используйте форму **no**, чтобы удалить заданные настройки.

```
monitor session SESSION-NUMBER source remote vlan VLAN-ID
no monitor session SESSION-NUMBER source remote vlan
```

Параметры

<i>SESSION-NUMBER</i>	Укажите номер сессии мониторинга. Доступный диапазон значений: от 1 до 4.
<i>VLAN-ID</i>	Укажите VLAN, через которую туннелируются отслеживаемые пакеты источника (source) с удаленного сайта. Доступный диапазон значений: от 2 до 4094.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду на коммутаторе назначения сессии RSPAN.

Команда **monitor session source remote vlan** применяется для настройки VLAN, на которую туннелируются отслеживаемые пакеты источника с удаленного сайта. Используйте команду **monitor session destination interface**, чтобы настроить порт назначения, на который будут переданы отслеживаемые пакеты.

Каждую сессию необходимо сконфигурировать с уникальной RSPAN VLAN. Используйте команду **remote-span** в режиме VLAN Configuration Mode, чтобы указать VLAN в качестве RSPAN VLAN.

Пример

В данном примере показано, как создать сессию RSPAN на коммутаторе назначения. VLAN 100 указана в качестве RSPAN VLAN, а порт Ethernet 1/0/4 указан в качестве порта назначения. Отслеживаемые пакеты прибывают на порт Ethernet 2/0/1 и будут переданы с порта Ethernet 1/0/4.

```
Switch# configure terminal
Switch(config)# vlan 100
Switch(config-vlan)# remote-span
Switch(config-vlan)# exit
Switch(config)# interface ethernet 2/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 100
Switch(config-if)# exit
Switch(config)# interface ethernet 1/0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
Switch(config-if)# exit
Switch(config)# monitor session 2 source remote vlan 100
Switch(config)# monitor session 2 destination interface ethernet 1/0/4
Switch(config)#
```

55-6 monitor session source vlan

Данная команда используется для того, чтобы настроить VLAN для мониторинга на основе VLAN. Используйте форму **no**, чтобы удалить VLAN из мониторинга на основе VLAN.

```
monitor session SESSION-NUMBER source vlan VLAN-ID [, | -] rx
no monitor session SESSION-NUMBER source vlan VLAN-ID [, | -]
```

Параметры

<i>SESSION-NUMBER</i>	Укажите номер сессии мониторинга. Доступный диапазон значений: от 1 до 4.
<i>VLAN-ID</i>	Укажите, чтобы сконфигурировать VLAN ID для мониторинга на основе VLAN. Доступный диапазон значений: от 1 до 4094.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
rx	Укажите, чтобы отслеживать пакеты, полученные на VLAN.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Для одной сессии мониторинга можно указать несколько VLAN, однако одну VLAN нельзя сконфигурировать в качестве VLAN источника (source) нескольких сессий. При указании параметра rx будут зеркалироваться все входящие пакеты на указанном VLAN ID.

Пример

В данном примере показано, как создать сессию мониторинга с номером 2. В качестве VLAN источника мониторинга указаны три VLAN: VLAN 2, VLAN 3 и VLAN 4.

```
Switch# configure terminal
Switch(config)# monitor session 2 destination interface ethernet 1/0/1
Switch(config)# monitor session 2 source vlan 2-4 rx
Switch(config)#
```

55-7 remote-span

Данная команда используется для указания VLAN в качестве RSPAN VLAN. Используйте форму no, чтобы вернуться к non-RSPAN VLAN.

remote-span
no remote-span

Параметры

Нет

По умолчанию

По умолчанию используется 802.1Q VLAN.

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду **remote-span** в режиме VLAN Configuration Mode, чтобы указать VLAN в качестве RSPAN VLAN. Если VLAN указана в качестве RSPAN VLAN, опция изучения MAC-адреса на RSPAN VLAN отключена. Используйте данную команду на любом из промежуточных коммутаторов и коммутаторе назначения (destination), участвующем в сессии RSPAN.

Для промежуточных коммутаторов, участвующих в сессии RSPAN, порт, на который прибывают отслеживаемые пакеты, и порт, с которого отправляются отслеживаемые пакеты, необходимо сконфигурировать в качестве тегированных портов-членов RSPAN VLAN.

Пример

В данном примере показано, как назначить VLAN 100 в качестве RSPAN VLAN на промежуточном коммутаторе в сессии RSPAN. Отслеживаемые пакеты прибывают на интерфейс Ethernet 1/0/1, а отправляются с интерфейса Ethernet 1/0/5.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 100
Switch(config-if)# exit
Switch(config)# interface ethernet 1/0/5
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 100
Switch(config-if)# exit
Switch(config)# vlan 100
Switch(config-vlan)# remote-span
Switch(config-vlan)#
```

55-8 no monitor session

Данная команда используется для удаления сессии мониторинга.

no monitor session *SESSION-NUMBER*

Параметры

SESSION-NUMBER

Укажите номер сессии мониторинга, которую необходимо

удалить. Доступный диапазон значений: от 1 до 4.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

При удалении сессии мониторинга будут удалены все настройки сессии.

Пример

В данном примере показано, как удалить сессию мониторинга с номером 1.

```
Switch# configure terminal
Switch(config)# no monitor session 1
Switch(config)#
```

55-9 show monitor session

Данная команда используется для отображения указанной сессии / всех сессий мониторинга.

show monitor session [SESSION-NUMBER | remote | local]

Параметры

<i>SESSION-NUMBER</i>	(Опционально) Укажите номер сессии, которую необходимо отобразить.
remote	(Опционально) Укажите, чтобы отобразить удаленную сессию RSPAN.
local	(Опционально) Укажите, чтобы отобразить локальную сессию.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду без указания номера сессии, чтобы отобразить все сессии мониторинга.

Пример

В данном примере показано, как отобразить сессию мониторинга порта с номером 1.

```
Switch#show monitor session

Session 1
  Session Type: local session
  Destination Port: Ethernet 1/0/1
  Source Ports:
    Both:
      Ethernet 1/0/2
      Ethernet 1/0/3
      Ethernet 1/0/4

Total Entries: 1

Switch#
```

56. Команды Multicast Listener Discovery (MLD) Snooping

56-1 clear ipv6 mld snooping statistics

Данная команда используется для сброса счетчиков статистики MLD Snooping на коммутаторе.

```
clear ipv6 mld snooping statistics {all | vlan VLAN-ID | interface INTERFACE-ID}
```

Параметры

all	Укажите, чтобы очистить статистику IPv6 MLD Snooping для всех VLAN и портов.
vlan VLAN-ID	Укажите VLAN. Если VLAN не указана, будет очищена статистика всех VLAN.
interface INTERFACE-ID	Укажите интерфейс.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы сбросить счетчики статистики MLD Snooping на коммутаторе.

Пример

В данном примере показано, как очистить всю статистику MLD Snooping.

```
Switch# clear ipv6 mld snooping statistics all
Switch#
```

56-2 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

Interface Configuration Mode
Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Чтобы применить MLD Snooping на VLAN, необходимо включить глобальное состояние MLD Snooping и MLD Snooping на интерфейсе. Настройки IGMP Snooping и MLD Snooping являются независимыми, поэтому их можно включать одновременно на одной и той же VLAN.

Пример

В данном примере показано, как отключить MLD Snooping на всех VLAN.

```
Switch# configure terminal
Switch(config)# no ipv6 mld snooping
Switch(config)#
```

В данном примере показано, как включить MLD Snooping на VLAN, доступных для данной функции.

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping
Switch(config)#
```

В данном примере показано, как включить MLD Snooping на VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping
Switch(config-vlan)#
```

56-3 ipv6 mld snooping access-group

Данная команда используется для того, чтобы разрешить получателям в рамках подсети подписываться только на те многоадресные группы, которые внесены в стандартный список доступа IPv6. Используйте форму **no**, чтобы отключить данную функцию.

```
ipv6 mld snooping access-group IPV6-ACCESS-LIST-NAME [vlan VLAN-ID]
no ipv6 mld snooping access-group [vlan VLAN-ID]
```


Параметры

<i>IPV6-ACCESS-LIST-NAME</i>	Укажите стандартный список доступа IPv6. Чтобы разрешить пользователям подписываться на группу (*, G), укажите «any» в поле адреса источника (source) и «G» в поле адреса назначения (destination) записи списка доступа.
vlan <i>VLAN-ID</i>	(Опционально) Укажите VLAN уровня 2. Будет включена фильтрация пакетов, прибывающих на VLAN.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы разрешить получателю многоадресного трафика подписываться только на указанные группы. Адрес назначения в списке доступа представляет собой адрес многоадресной группы, используемый для того, чтобы разрешить/запретить получателю подписываться на многоадресную группу.

Данная команда используется для конфигурирования физических портов или port-channel.

Пример

В данном примере показано, как разрешить интерфейсу Ethernet 1/0/1 подписаться только на группу FF1E::14. Сначала создается список доступа IPv6 «mld_filter», разрешающий только пакеты, предназначенные для группы с адресом FF1E::14. Затем группа доступа «mld_filter» ассоциируется с интерфейсом Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#ipv6 access-list mld_filter
Switch(config-ipv6-acl)#permit any host FF1E::14
Switch(config-ipv6-acl)#end
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#ipv6 mld snooping access-group mld_filter
Switch(config-if)#
```

56-4 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

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Используйте команду **ipv6 mld snooping fast-leave**, чтобы удалить принадлежность MLD с порта сразу же после получения сообщения Leave, не используя механизм запросов Group-Specific или Group-and-Source-Specific Query.

Пример

В данном примере показано, как включить функцию MLD Snooping Fast Leave на VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping fast-leave
Switch(config-vlan)#
```

56-5 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

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Получив сообщение Done, MLD Snooping Querier считает, что на интерфейсе больше нет локальных участников, если после истечения времени ответа не пришло ни одно сообщение. Уменьшив данный интервал, можно сократить количество времени, которое требуется маршрутизатору для обнаружения потери последнего участника группы.

Пример

В данном примере показано, как настроить интервал Last Listener Query. Указанное значение – 3 секунды.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping last-listener-query-interval 3
Switch(config-vlan)#
```

56-6 ipv6 mld snooping limit

Данная команда используется для указания максимального количества многоадресных групп или каналов MLD Snooping, на которые может подписаться интерфейс уровня 2. Используйте форму **no**, чтобы удалить данное ограничение.

```
ipv6 mld snooping limit NUMBER [exceed-action {drop | replace}] [except IPv6-ACCESS-LIST-NAME]
[vlan VLAN-ID]
no ipv6 mld snooping limit [vlan VLAN-ID]
```

Параметры

NUMBER	Укажите максимальное количество групп MLD Snooping, на которые может подписаться интерфейс. Доступный диапазон значений: от 1 до 4096.
exceed-action	(Опционально) Укажите действие, которое необходимо применить к новым группам после превышения максимального количества групп.
drop	(Опционально) Укажите, чтобы отбросить новую группу.
replace	(Опционально) Укажите, чтобы заменить старую группу новой.
except <i>IPv6-ACCESS-LIST-NAME</i>	(Опционально) Укажите стандартный список доступа IPv6. С группы (*,G) или канала (S,G), внесенных в список доступа, будут сняты ограничения по максимальному количеству. Чтобы разрешить канал (S,G), укажите «S» в поле адреса источника (source) и «G» в поле адреса назначения (destination) записи списка доступа. Чтобы разрешить группу (*,G), укажите «any» в поле адреса источника и «G» в поле адреса назначения записи списка доступа.

vlan <i>VLAN-ID</i>	(Опционально) Укажите VLAN уровня 2. Будет включена фильтрация пакетов, прибывающих на данную VLAN.
----------------------------	---

По умолчанию

По умолчанию количество групп не ограничено.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для конфигурирования физических портов и port-channel.

Пример

В данном примере показано, как указать максимальное количество групп MLD Snooping, на которые может подписаться интерфейс Ethernet 1/0/4 с VLAN ID 1000, а также как снять ограничение по количеству со списка доступа «mld_filter».

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/4
Switch(config-if)# ipv6 mld snooping limit 80 except mld_filter vlan 1000
Switch(config-if)#
```

В данном примере показано, как удалить ограничение по количеству для групп MLD Snooping, на которые может подписаться интерфейс port-channel 4 с VLAN ID 1000.

```
Switch# configure terminal
Switch(config)# interface port-channel 4
Switch(config-if)# no ipv6 mld snooping limit vlan 1000
Switch(config-if)#
```

56-7 ipv6 mld snooping mrouter

Данная команда используется для того, чтобы настроить указанный интерфейс в качестве порта IPv6, подключенного к многоадресному маршрутизатору, или порта, которому запрещено подключаться к многоадресному маршрутизатору, на интерфейсе VLAN. Используйте форму **no**, чтобы удалить интерфейс из списка портов, подключенных к маршрутизатору, или портов, которым запрещено подключаться к многоадресному маршрутизатору.

```
ipv6 mld snooping mrouter {interface INTERFACE-ID [, | -] | forbidden interface INTERFACE-ID [, | -] |
learn pimv6}
no ipv6 mld snooping mrouter {interface INTERFACE-ID [, | -] | forbidden interface INTERFACE-ID [, | -]
| learn pimv6}
```

Параметры

interface	Укажите диапазон интерфейсов, подключенных к многоадресным маршрутизаторам.
forbidden interface	Укажите диапазон интерфейсов, не подключенных к многоадресным маршрутизаторам.
<i>INTERFACE-ID</i>	Укажите интерфейс или список интерфейсов. Пробелы до и после запятой недопустимы. Доступны физические интерфейсы или port-channel.
learn pimv6	Укажите, чтобы включить динамическое изучение на портах, подключенных к многоадресному маршрутизатору.

По умолчанию

Порт IPv6, подключенный к многоадресному маршрутизатору, не настроен. Автоматическое изучение включено.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. В качестве порта, подключенного к многоадресному маршрутизатору, можно использовать физический порт или port-channel. Указанный порт должен являться портом-членом сконфигурированной VLAN. Нельзя указать порт-член port-channel.

Порт, подключенный к многоадресному маршрутизатору, может быть изучен динамически или сконфигурирован статически на устройстве с включенной функцией MLD Snooping. При динамическом изучении устройство MLD Snooping будет анализировать пакеты MLD и PIMv6, чтобы выяснить, является ли связанное устройство маршрутизатором.

Пример

В данном примере показано, как сконфигурировать интерфейс Ethernet 1/0/1 в качестве 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)#
```

56-8 ipv6 mld snooping ignore-topology-change-notification

Данная команда используется для того, чтобы функция MLD Snooping игнорировала изменения STP и не отправляла запрос STP на интерфейсе. Используйте форму **no**, чтобы функция MLD Snooping не игнорировала изменения STP и отправляла запрос STP на указанном интерфейсе.

ipv6 mld snooping ignore-topology-change-notification
no ipv6 mld snooping ignore-topology-change-notification

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Коммутатор с включенной функцией MLD Snooping осведомлен об изменениях топологии Link Layer, вызванных применением Spanning Tree. Если порт включен/отключен при помощи Spanning Tree, сообщение General Query будет отправлено на все активные порты, не подключенные к маршрутизатору, чтобы сократить время сетевой конвергенции. Используйте данную команду, чтобы функция MLD Snooping игнорировала изменения топологии.

Пример

В данном примере показано, как включить игнорирование функцией MLD Snooping изменений топологии на VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping ignore-topology-change-notification
Switch(config-vlan)#
```

56-9 ipv6 mld snooping proxy-reporting

Данная команда используется для включения функции Proxy Reporting. Используйте форму **no**, чтобы отключить данную функцию.

```
ipv6 mld snooping proxy-reporting [source IPV6-ADDRESS]
no ipv6 mld snooping proxy-reporting
```

Параметры

source IPV6-ADDRESS	(Опционально) Укажите IP-адрес источника (source) Proxy Reporting.
----------------------------	--

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Функция Proxy Reporting работает только для трафика MLDv1.

Если функция Proxy Reporting включена, несколько полученных пакетов MLD Report или MLD Leave будут объединены в одно сообщение, а затем отправлены на порт, подключенный к маршрутизатору. IP-адрес источника Proxy Reporting будет использован в качестве IP-адреса источника сообщения.

Если IP-адрес источника Proxy Reporting не указан, будет использован нулевой IP-адрес. MAC-адрес интерфейса будет использован в качестве MAC-адреса источника сообщения. Если для VLAN не указан IP-адрес, будет использован системный MAC-адрес.

Пример

В данном примере показано, как включить MLD Snooping Proxy Reporting на VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping proxy-reporting
Switch(config-vlan)#
```

56- 10 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

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Чтобы запустить MLD Snooping Querier, интерфейсу необходимо предварительно присвоить IPv6-адрес. При отсутствии у VLAN IPv6-адреса будет выслано сообщение Warning. Если Querier включен, а IPv6-адрес удален, работа Querier будет приостановлена.

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)#
```

56- 11 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

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Интервал MLD General Query – это промежуток времени между запросами General Query, отправляемыми Querier. Изменяя данный интервал, можно настроить количество сообщений MLD в сети. Чем больше значение интервала, тем реже будут отправляться сообщения MLD Query.

Пример

В данном примере показано, как настроить интервал MLD Snooping Query на VLAN 1000. Указанное значение – 300 секунд.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping query-interval 300
Switch(config-vlan)#
```

56- 12 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

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Команда применяется для настройки периода времени, в течение которого участник группы может ответить на сообщение MLD Query. После истечения данного периода его участие в группе будет удалено.

Пример

В данном примере показано, как настроить максимальное время ответа на интерфейсе. Указанное значение – 20 секунд.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping query-max-response-time 20
Switch(config-vlan)#
```

56- 13 ipv6 mld snooping query-version

Данная команда используется для того, чтобы настроить версию пакета General Query, отправленного MLD Snooping Querier. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ipv6 mld snooping query-version {1 | 2}
no ipv6 mld snooping query-version

Параметры

1	Укажите версию пакета MLD General Query, отправленного MLD Snooping Querier – 1.
2	Укажите версию пакета MLD General Query, отправленного MLD Snooping Querier – 2.

По умолчанию

Версия по умолчанию – 2.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN.

Пример

В данном примере показано, как указать версию Query на VLAN 1000. Указанная версия – 1.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping query-version 1
Switch(config-vlan)#
```

56- 14 ipv6 mld snooping rate-limit

Данная команда используется для настройки максимального количества входящих пакетов MLD Control в секунду. Используйте форму **no**, чтобы отключить данное ограничение.

```
ipv6 mld snooping rate-limit NUMBER
no ipv6 mld snooping rate-limit
```

Параметры

<i>NUMBER</i>	Укажите максимальное количество пакетов MLD Control, обрабатываемых коммутатором на указанном интерфейсе в секунду.
---------------	---

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для конфигурирования интерфейса VLAN, физических портов или port-channel. Используйте данную команду, чтобы указать максимальное количество пакетов MLD Control, обрабатываемых на интерфейсе в секунду.

Пример

В данном примере показано, как указать максимальное количество пакетов на интерфейсе VLAN 1000 в секунду. Указанное значение – 30 пакетов.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping rate-limit 30
Switch(config-vlan)#
```

56- 15 ipv6 mld snooping report-suppression

Данная команда используется для включения функции MLD Report Suppression на VLAN. Используйте форму **no**, чтобы отключить MLD Report Suppression на VLAN.

```

ipv6 mld snooping report-suppression
no ipv6 mld snooping report-suppression

```

Параметры

Нет

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Функция Report Suppression работает только для трафика MLDv1.

Если функция Report Suppression включена, коммутатор блокирует дублированные сообщения, отправленные узлами. Дублированные сообщения Report или Leave для одной группы будут блокироваться до тех пор, пока не истечет время блокировки. Будет передано только одно сообщение Report или Leave, остальные сообщения будут заблокированы.

Пример

В данном примере показано, как включить функцию MLD Report Suppression.

```

Switch# configure terminal
Switch(config)# vlan 100
Switch(config-vlan)# ipv6 mld snooping report-suppression
Switch(config-vlan)#

```

56- 16 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

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN.

Robustness variable обеспечивает точную настройку в соответствии с ожидаемой потерей пакетов на интерфейсе. Значение robustness variable используется для вычисления следующих интервалов сообщений MLD:

- Group member interval – промежуток времени, по истечении которого маршрутизатор считает, что в группе больше нет активных участников. Данный интервал рассчитывается следующим образом: (robustness variable x query interval) + (1 x query response interval).
- Other querier present interval – промежуток времени, по истечении которого многоадресный маршрутизатор считает, что маршрутизатор, являющийся Querier, больше не доступен. Данный интервал рассчитывается следующим образом: (robustness variable x query interval) + (0,5 x query response interval).
- Last member query count – количество запросов Group-Specific Query, отправленных маршрутизатором до того, как он предполагает, что в группе нет локальных участников. Количество по умолчанию равно значению robustness variable.

Данное значение может быть увеличено, если в подсети ожидается потеря пакетов.

Пример

В данном примере показано, как сконфигурировать значение robustness variable на интерфейсе VLAN 1000. Указанное значение – 3.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping robustness-variable 3
Switch(config-vlan)#
```

56-17 ipv6 mld snooping static-group

Данная команда используется для настройки статической группы MLD Snooping. Используйте форму **no**, чтобы удалить статическую группу.

```
ipv6 mld snooping static-group IPV6-ADDRESS interface INTERFACE-ID [, | -]
no ipv6 mld snooping static-group IPV6-ADDRESS [interface INTERFACE-ID [, | -]]
```

Параметры

IPV6-ADDRESS

Укажите IPv6-адрес многоадресной группы.

interface <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

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Используйте данную команду на интерфейсе VLAN, чтобы статически добавить записи об участии в группе и/или записи источника (source).

Используйте команду **ipv6 mld snooping static-group**, чтобы создать статическую группу MLD Snooping, если прикрепленный узел не поддерживает протокол MLD .

Пример

В данном примере показано, как статически добавить группу и/или запись источника для MLD Snooping.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping static-group FF02::12:03 interface ethernet 1/0/5
Switch(config-vlan)#
```

56- 18 ipv6 mld snooping suppression-time

Данная команда используется для того, чтобы настроить время блокирования дублированных сообщений MLD Report или MLD Leave. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ipv6 mld snooping suppression-time *SECONDS*
no ipv6 mld snooping suppression-time

Параметры

<i>SECONDS</i>	Укажите, чтобы настроить время блокирования дублированных сообщений MLD Report. Доступный диапазон значений: от 1 до 300.
----------------	---

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Функция Report Suppression будет блокировать дублированные пакеты MLD Report или MLD Leave, полученные в течение времени блокирования. Чем меньше время блокирования, тем чаще будут отправляться дублированные пакеты MLD.

Пример

В данном примере показано, как настроить время блокирования на VLAN 1000. Указанное значение – 125.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping suppression-time 125
Switch(config-vlan)#
```

56-19 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

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда доступна только для конфигурирования интерфейса VLAN. Данные настройки применимы только для фильтрации сообщений об участии MLD.

Пример

В данном примере показано, как ограничить подключение всех узлов MLDv1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping minimum-version 2
Switch(config-vlan)#
```

56-20 show ipv6 mld snooping

Данная команда используется для отображения информации об MLD Snooping на коммутаторе.

show ipv6 mld snooping [vlan VLAN-ID]

Параметры

vlan VLAN-ID	(Опционально) Укажите VLAN, которую необходимо отобразить.
---------------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Если не указаны дополнительные параметры, будет отображена информация об MLD Snooping для всех VLAN, на которых включена данная функция.

Пример

В данном примере показано, как отобразить настройки MLD Snooping.


```

Switch# show ipv6 mld snooping

MLD snooping global state: Enabled

VLAN #1 configuration
  MLD snooping state      : Enabled
  Minimum version        : v2
  Fast leave              : Enabled (host-based)
  Report suppression     : Enabled
  Suppression time       : 10 seconds
  Proxy Reporting        : Disabled
  Mrouter port learning  : Enabled
  Querier state          : Enabled (Non-active)
  Query version          : v2
  Query interval         : 125
  Max response time      : 10 seconds
  Robustness value       : 2
  Last listener query interval : 1 second
  Rate limit             : 50
  Ignore topology change : Disabled

Total Entries: 1

Switch#

```

56-21 show ipv6 mld snooping filter

Данная команда используется для отображения информации о фильтре MLD Snooping на указанных интерфейсах.

```
show ipv6 mld snooping filter [interface INTERFACE-ID [, | -]]
```

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите интерфейсы физических портов или port-channel, которые необходимо отобразить.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию об ограничениях и группе доступа MLD Snooping. Если не указаны дополнительные параметры, будет отображена информация о фильтре MLD Snooping для всех интерфейсов.

Пример

В данном примере показано, как отобразить информацию о фильтре, не указывая конкретный интерфейс.

```
Switch# show ipv6 mld snooping filter

eth1/0/1:
  Rate limit: 30pps
  Access group: mld_filter
  Groups/Channel Limit: Not Configured
  vlan 1:
    Access group: Not Configured
    Groups/Channel Limit: 25 (Exception List: mld_filter, exceed-action: drop)

eth1/0/3:
  Rate limit: 20pps
  Access group: mld_filter
  Groups/Channel Limit: Not Configured
  vlan 1:
    Access group: mld_filter
    Groups/Channel Limit: Not Configured
  vlan 2:
    Access group: Not Configured
    Groups/Channel Limit: 100 (exceed-action: replace)

port-channel4:
  Rate limit: 200pps
  Access group: Not Configured
  Groups/Channel Limit: Not Configured

Switch#
```

56-22 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] [detail]
```

Параметры

<i>IPV6-ADDRESS</i>	(Опционально) Укажите IP-адрес группы. Если IPv6-адрес не указан, будет отображена информация обо всех группах MLD Snooping.
vlan <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.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
detail	(Опционально) Укажите, чтобы отобразить подробную информацию о группе MLD Snooping.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию о группе MLD Snooping.

Пример

В данном примере показано, как отобразить информацию о группе MLD Snooping.

```
Switch# show ipv6 mld snooping groups

Total Group Entries : 1
Total Source Entries: 1

vlan 1, FF1E::1
Learned on port: 1/0/3

Switch#
```

56-23 show ipv6 mld snooping mrouter

Данная команда используется для того, чтобы отобразить информацию об автоматически изученном или настроенном вручную многоадресном маршрутизаторе MLD Snooping.

show ipv6 mld snooping mrouter [vlan VLAN-ID [, | -]]**Параметры**

vlan VLAN-ID	(Опционально) Укажите VLAN ID, который необходимо отобразить. Если VLAN не указана, будет отображена информация о многоадресном маршрутизаторе MLD Snooping на всех VLAN.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить интерфейсы динамически изученного или сконфигурированного вручную многоадресного маршрутизатора.

Пример

В данном примере показано, как отобразить информацию о многоадресном маршрутизаторе MLD Snooping.

```
Switch#show ipv6 mld snooping mrouter

VLAN  Ports
-----
1      1/0/3, 1/0/4 (static)
        1/0/6 (forbidden)
        1/0/7 (dynamic)

3      1/0/8 (static)
        1/0/9 (dynamic)

Total Entries: 2

Switch#
```

56-24 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.
vlan <i>VLAN-ID</i>	(Опционально) Укажите VLAN ID, который необходимо отобразить.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения статически сконфигурированных групп MLD Snooping на коммутаторе. Если не указаны дополнительные параметры, будет отображена вся информация.

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                                       1/0/1-1/0/2

Total Entries: 1

Switch#
```

56-25 show ipv6 mld snooping statistics

Данная команда используется для отображения статистики MLD Snooping на коммутаторе.

show ipv6 mld snooping statistics {**interface** [*INTERFACE-ID* [, | -]] | **vlan** [*VLAN-ID* [, | -]]}

Параметры

interface	Укажите, чтобы отобразить счетчики статистики для интерфейса.
<i>INTERFACE-ID</i>	(Опционально) Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
vlan	Укажите, чтобы отобразить счетчики статистики для VLAN.
<i>VLAN-ID</i>	(Опционально) Укажите VLAN ID, который необходимо отобразить.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить статистику MLD Snooping.

Пример

В данном примере показано, как отобразить статистику MLD Snooping.

```
Switch#show ipv6 mld sn statistics interface

Interface eth1/0/4
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Interface eth1/0/7
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Interface eth1/0/8
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Total Entries: 3

Switch#show ipv6 mld sn statistics vlan 1

Switch#show ipv6 mld sn statistics vlan 20

VLAN 20 Statistics:
  Rx: v1Report 0, v2Report 0, Query 953, v1Done 0
  Tx: v1Report 667, v2Report 1, Query 996, v1Done 0

Total Entries: 1

Switch#
```

57. Команды Multicast VLAN

57-1 mvlan enable

Данная команда используется для включения функции Multicast VLAN и настройки некоторых ее параметров. Используйте форму **no**, чтобы отключить функцию и вернуться к настройкам по умолчанию.

```
mvlan {ipv4 enable | ipv6 enable}
no mvlan {ipv4 enable | ipv6 enable}
```

Параметры

ipv4 enable	Укажите, чтобы включить функцию Multicast VLAN для многоадресных IPv4-пакетов.
ipv6 enable	Укажите, чтобы включить функцию Multicast VLAN для многоадресных IPv6-пакетов.

По умолчанию

По умолчанию Multicast VLAN для IPv4/IPv6-пакетов отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения/отключения функции Multicast VLAN и настройки некоторых ее параметров.

Пример

В данном примере показано, как включить функцию Multicast VLAN для многоадресных IPv4-пакетов.

```
Switch# configure terminal
Switch(config)# mvlan ipv4 enable
Switch(config)#
```

57-2 mvlan

Данная команда используется для настройки характеристик функции Multicast VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
mvlan {forward-unmatched | ignore-vlan}
no mvlan {forward-unmatched | ignore-vlan}
```

Параметры

forward-unmatched	Укажите, чтобы полученные управляющие IGMP или MLD-пакеты были перенаправлены или отброшены, если они нетегированные или не соответствуют ни одному профилю. VLAN, используемая для привязки по умолчанию, или является Multicast VLAN, или будет помечена тегом Multicast VLAN, не соответствующей привязанному профилю.
ignore-vlan	Укажите, чтобы настроить тегированные управляющие IGMP или MLD- пакеты. Если данная функция включена, коммутатор проигнорирует VLAN полученных управляющих IGMP/MLD-пакетов или попытается найти соответствующий профиль.

По умолчанию

По умолчанию параметр **forward-unmatched** отключен, а пакеты отбрасываются.
По умолчанию параметр **ignore-vlan** отключен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Нетегированный IGMP/MLD-пакет (Report/Leave/Done), полученный портом, будет проверен на соответствие профилю группы Multicast VLAN, к которой принадлежит данный порт. При соответствии пакет будет принадлежать соответствующей Multicast VLAN и обработан с помощью процесса изучения последующей группы с соответствующей Multicast VLAN.

Если пакет не соответствует ни одной Multicast VLAN, или если привязанная к пакету VLAN является Multicast VLAN, IGMP/MLD-пакет будет отброшен или перенаправлен на Member-порты VLAN в зависимости от настройки параметра **forward-unmatched**. При указании **no mvlan forward-unmatched** пакет будет отброшен, а при указании **mvlan forward-unmatched** пакет будет перенаправлен.

Если пакет не соответствует ни одной Multicast VLAN и VLAN пакета не настроена в качестве Multicast VLAN, то IGMP/MLD-пакет не будет обработан Multicast VLAN.

Если IGMP/MLD-пакет (Report/Leave/Done), полученный портом, тегированный, то обработка осуществляется в зависимости от настройки параметра **ignore-vlan**.

Пакет, соответствующий профилю группы VLAN, и VLAN которого является Multicast VLAN, обрабатывается с помощью процесса изучения последующей группы. Если соответствия отсутствуют, пакет отбрасывается в зависимости от настройки параметра **forward-unmatched**. Пакет, VLAN которого не является Multicast VLAN, не будет обработан Multicast VLAN.

Если IGMP/MLD Snooping включена для VLAN пакета, для него будут действовать правила данной функции. Если IGMP/MLD Snooping отключена, VLAN игнорируется и будет использован привязанный к порту профиль группы Multicast VLAN. При найденном соответствии пакет будет обработан с помощью процесса изучения последующей группы с соответствующей Multicast VLAN. Если соответствия отсутствуют, но VLAN пакета

является Multicast VLAN, пакет будет обработан на основе настроек параметра **forward-unmatched**. Пакет, VLAN которого не является Multicast VLAN, не будет обработан Multicast VLAN.

Пример

В данном примере показано, как включить параметр **forward-unmatched** и проигнорировать настройки VLAN.

```
Switch# configure terminal
Switch(config)# mvlan forward-unmatched
Switch(config)# mvlan ignore-vlan
Switch(config)#
```

57-3 mvlan vlan

Данная команда используется для создания Multicast VLAN. Используйте форму **no**, чтобы удалить Multicast VLAN.

```
mvlan vlan VLAN-ID
no mvlan vlan VLAN-ID
```

Параметры

VLAN-ID	Укажите Multicast VLAN. Доступный диапазон значений: от 1 до 4094.
---------	--

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

VLAN, созданная в качестве обычной 802.1Q VLAN, не может быть указана в качестве Multicast VLAN, и наоборот. Включить GMP/MLD Snooping для VLAN и указать ее в качестве Multicast VLAN одновременно нельзя.

Пример

В данном примере показано, как создать Multicast VLAN 100.

```
Switch# configure terminal
Switch(config)# mvlan ipv4 enable
Switch(config)# mvlan vlan 100
Switch(config-mvlan)#
```

57-4 member

Данная команда используется для настройки интерфейсов в качестве портов source (источник) или reciever (получатель) для Multicast VLAN. Используйте форму **no**, чтобы удалить порты source и reciever.

```
member {receiver | source} {tagged | untagged} INTERFACE-ID [, | -]  
no member {receiver | source} INTERFACE-ID [, | -]
```

Параметры

receiver	Укажите, чтобы настроить порт в качестве абонентского порта, который может только получать данные многоадресной рассылки в Multicast VLAN.
source	Укажите, чтобы настроить порт в качестве порта Uplink, который может отправлять данные многоадресной рассылки в Multicast VLAN.
tagged	Укажите, чтобы пакеты, отправленные тегированным портом, были помечены Multicast VLAN ID.
untagged	Укажите, чтобы пакеты, отправленные нетегированным портом, были перенаправлены без тега.
INTERFACE-ID	Укажите интерфейсы, которые необходимо использовать.
,	(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 ни один из портов source или reciever не является членом какой-либо Multicast VLAN.

Режим ввода команды

Multicast VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Member-порт Multicast VLAN может выступать в качестве порта source (источник), из которого отправляется многоадресный трафик, и в качестве порта reciever (получатель), подключенного к абонентам.

Multicast VLAN может иметь более одного порта source. Если IGMP/MLD-пакеты Report поступают из порта source, Multicast VLAN не будет изучать IGMP/MLD-группу для данного Report, а перенаправит пакеты на другие порты source в Multicast VLAN.

Порт может быть портом reciever для нескольких VLAN одновременно.

Ниже перечислены некоторые ограничения при настройке порта source или reciever для Multicast VLAN:

- Порт не может быть портом source и reciever одновременно в одной Multicast VLAN.

- Порты source в одной Multicast VLAN должны быть все либо с тегом, либо все без тега.
- Тегированные порты reciever не должны совпадать с нетегированными портами reciever в одной Multicast VLAN.
- Порты source в одной Multicast VLAN не должны совпадать с портами reciever между двумя Multicast VLAN.
- Тегированные порты source не должны совпадать с нетегированными портами source между двумя Multicast VLAN.

Пример

В данном примере показано, как настроить Ethernet-порты от 1/0/1 до 1/0/4 в качестве тегированных портов reciever в Multicast VLAN 100.

```
Switch#configure terminal
Switch(config)#mvlan vlan 100
Switch(config-mvlan)#member receiver tagged ethernet 1/0/1-4
Switch(config-mvlan)#
```

57-5 name

Данная команда используется для указания имени Multicast VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
name VLAN-NAME
no name
```

Параметры

<i>VLAN-NAME</i>	Укажите имя VLAN. Максимально допустимое количество символов – 32.
------------------	--

По умолчанию

По умолчанию именем VLAN является MVLANxxxx, где xxxx – четыре цифры (включая начальные нули), которые равны VLAN ID.

Режим ввода команды

Multicast VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для указания имени Multicast VLAN.

Пример

В данном примере показано, как настроить имя для Multicast VLAN 100. Настроенное имя – ip-tv.

```
Switch# configure terminal
Switch(config)# mvlan vlan 100
Switch(config-mvlan)# name ip-tv
Switch(config-mvlan)#
```

57-6 replace-source-ip

Данная команда используется для замены IP-адреса источника в IGMP/MLD-пакетах Report, отправленных на порты Uplink. Используйте форму **no**, чтобы отменить замену.

replace-source-ip {ipv4 IPV4-ADDRESS | ipv6 IPV6-ADDRESS} from {source | receiver | both}
no replace-source-ip {ipv4 | ipv6}

Параметры

ipv4 IPV4-ADDRESS	Укажите IP-адрес источника, который необходимо использовать для замены в управляющих IGMP-пакетах Report на портах Uplink.
ipv6 IPV6-ADDRESS	Укажите IP-адрес источника, который необходимо использовать для замены в управляющих MLD-пакетах Report на портах Uplink.
source	Укажите IPv4 или IPv6-адрес источника для замены в IGMP или MLD- пакетах Report/Leave/Done, полученных на любом из портов source в Multicast VLAN.
receiver	Укажите IPv4 или IPv6-адрес источника для замены в IGMP или MLD- пакетах Report/Leave/Done, полученных на любом из портов receiver в Multicast VLAN.
both	Укажите IPv4 или IPv6-адрес источника для замены в IGMP или MLD- пакетах Report/Leave/Done, полученных на любом из портов Multicast VLAN.

По умолчанию

Нет

Режим ввода команды

Multicast VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для передачи информации о подключениях к порту source во избежание отбрасывания управляющих пакетов маршрутизатором Uplink во время проверок IP Spoofing.

Для изменения IP-адреса источника необходимо настроить его до того, как IGMP/MLD-пакеты Report/Leave/Done будут отправлены узлом. В противном случае IP-адрес не будет изменен.

Пример

В данном примере показано, как заменить IPv4-адрес и IPv6-адрес источника.

```
Switch#configure terminal
Switch(config)#mvlan vlan 100
Switch(config-mvlan)#replace-source-ip ipv4 1.10.10.10 from receiver
Switch(config-mvlan)#replace-source-ip ipv6 FE80:3000::3 from source
Switch(config-mvlan)#
```

57-7 mvlan group-profile

Данная команда используется для создания профиля группы для функции Multicast VLAN. Используйте форму **no**, чтобы удалить один или все профили группы.

```
mvlan group-profile PROFILE-NAME
no mvlan group-profile {PROFILE-NAME | all}
```

Параметры

<i>PROFILE-NAME</i>	Укажите имя профиля.
all	Укажите, чтобы удалить все профили Multicast VLAN.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Профиль используется для указания диапазонов адресов группы. Multicast VLAN проверяет адрес группы в IGMP/MLD-пакете на соответствие диапазону адресов, настроенному в указанном профиле.

Пример

В данном примере показано, как создать профиль под именем «mv_profile1».

```
Switch#configure terminal
Switch(config)#mvlan group-profile mv_profile1
Switch(config-mvlan-profile)#
```

57-8 access-group

Данная команда используется для привязки профиля группы доступа к Multicast VLAN. Используйте форму **no**, чтобы удалить привязку.

```
access-group PROFILE-NAME
no access-group PROFILE-NAME
```

Параметры

<i>PROFILE-NAME</i>	Укажите имя профиля.
---------------------	----------------------

По умолчанию

Нет

Режим ввода команды

Multicast VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

К одной Multicast VLAN могут быть привязаны несколько профилей в качестве действительных диапазонов групп, которые не должны совпадать с Multicast VLAN. Если порт является членом нескольких Multicast VLAN, для изучения группы будет выбрана Multicast VLAN, назначенная привязкой **group-profile**.

Если порт является членом одной Multicast VLAN и группа доступа настроена для Multicast VLAN, с помощью Multicast VLAN будут изучены только группы, разрешенные группой доступа. Если группа доступа не настроена, то с помощью Multicast VLAN будут изучены все группы многоадресной рассылки.

Пример

В данном примере показано, как привязать профиль «mv_profile1» к Multicast VLAN 100.

```
Switch#configure terminal
Switch(config)#mvlan vlan 100
Switch(config-mvlan)#access-group mv_profile1
Switch(config-mvlan)#
```

57-9 range

Данная команда используется для настройки диапазона многоадресных адресов для профиля Multicast VLAN. Используйте форму **no**, чтобы удалить диапазон.

```
range {IPV4-ADDRESS-START[IPV4-ADDRESS-END] | IPV6-ADDRESS-START[IPV6-ADDRESS-END]}
no range {IPV4-ADDRESS-START[IPV4-ADDRESS-END] | IPV6-ADDRESS-START[IPV6-ADDRESS-END]}
```

Параметры

<i>IPV4-ADDRESS-START</i>	Укажите начальный многоадресный IPv4-адрес в диапазоне.
---------------------------	---

<i>IPV4-ADDRESS-END</i>	Укажите конечный многоадресный IPv4-адрес в диапазоне.
<i>IPV6-ADDRESS-START</i>	Укажите начальный многоадресный IPv6-адрес в диапазоне.
<i>IPV6-ADDRESS-END</i>	Укажите конечный многоадресный IPv6-адрес в диапазоне.

По умолчанию

Нет

Режим ввода команды

Multicast VLAN Profile Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

В профиль Multicast VLAN могут быть добавлены несколько диапазонов. Диапазоны IP-адресов, указанные в одном профиле, должны быть в одном семействе адресов.

Пример

В данном примере показано, как добавить диапазон IPv4 в профиль под именем «profile mv_profile1».

```
Switch#configure terminal
Switch(config)#mvlan group-profile mv_profile1
Switch(config-mvlan-profile)#range 225.0.0.0 225.0.0.5
Switch(config-mvlan-profile)#
```

57-10 show mvlan group-profile

Данная команда используется для отображения настроек профиля группы многоадресной рассылки.

```
show mvlan group-profile [PROFILE-NAME]
```

Параметры

<i>PROFILE-NAME</i>	(Опционально) Укажите имя профиля.
---------------------	------------------------------------

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду без указания имени профиля, чтобы отобразить все профили группы.

Пример

В данном примере показано, как отобразить все профили Multicast VLAN.

```
Switch#show mvlan group-profile

Profile Name                Multicast Address
-----
mv_profile1                225.0.0.0 - 225.0.0.5

Total Entries: 1

Switch#
```

57-11 show mvlan access-group

Данная команда используется для отображения привязок профилей группы многоадресной рассылки к Multicast VLAN.

show mvlan access-group [VLAN-ID]

Параметры

VLAN-ID	(Опционально) Укажите VLAN ID.
---------	--------------------------------

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду без указания VLAN ID, чтобы отобразить информацию о всех привязках.

Пример

В данном примере показано, как отобразить профили группы, привязанные к Multicast VLAN.

```
Switch#show mvlan access-group
Multicast VLAN  Multicast Group Profiles
-----
100             mv_profile1

Total Entries: 1

Switch#
```

57-12 show mvlan

Данная команда используется для отображения настроек Multicast VLAN.

show mvlan [VLAN-ID]

Параметры

<i>VLAN-ID</i>	(Опционально) Укажите VLAN ID.
----------------	--------------------------------

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Если ни один из опциональных параметров не указан, будут отображены настройки и информация о всех Multicast VLAN.

Пример

В данном примере показано, как отобразить настройки и информацию о всех Multicast VLAN на коммутаторе.

```

Switch#show mvlan

IPv4 Multicast VLAN State      : Enabled
IPv6 Multicast VLAN State      : Disabled
Forward Unmatched              : Disabled
Ignore VLAN                    : Disabled

MVLAN 100
  Name                          : ip-tv
  Untagged Receiver             :
  Tagged Receiver               : 1/0/1-1/0/4
  Untagged Source               :
  Tagged Source                 :
  Replace Source IP             : 1.10.10.10 (from receiver)/FE80:3000::3 (from source)
  Replace Priority               : 4 (IPv4)/Not replace (IPv6)

Total Entries: 1

Switch#

```

Отображаемые параметры

IPv4 Multicast VLAN State	Включение функции Multicast VLAN для IPv4-пакетов.
IPv6 Multicast VLAN State	Включение функции Multicast VLAN для IPv6-пакетов.
Forward Unmatched	Режим Forwarding Mode для несоответствующих пакетов Multicast VLAN. Enabled означает, что несоответствующие пакеты будут перенаправлены. Disabled означает, что несоответствующие пакеты будут отброшены.
Ignore VLAN	Игнорирование тега VLAN управляющих IGMP-пакетов и их автоматическое назначение в корректной Multicast VLAN для обработки.
Untagged/Tagged Receiver/Source	Порты receiver или source, настроенные в Multicast VLAN, и тегированный или нетегированный атрибут VLAN для многоадресных пакетов, отправленных на данные порты.
Replace Source IP	IP-адрес источника, который будет использован для замены в управляющих IGMP/MLD-пакетах перед их отправкой в Multicast VLAN.
Replace Priority	Пакеты данных многоадресной рассылки, отправленные в Multicast VLAN, будут помечены указанным приоритетом.

58. Команды Neighbor Discovery (ND) Inspection

58-1 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы создать политику ND Inspection Policy и войти в режим ND Inspection Policy Configuration Mode. ND Inspection предназначена для проверки сообщений Neighbor Solicitation (NS) и Neighbor Advertisement (NA).

Пример

В данном примере показано, как создать политику ND под именем «policy1».

```
Switch# configure terminal
Switch(config)# ipv6 nd inspection policy policy1
Switch(config-nd-inspection)#
```

58-2 validate source-mac

Данная команда используется для проверки MAC-адреса на соответствие адресу Link Layer для ND-сообщений. Используйте форму **no**, чтобы отменить проверку.

```
validate source-mac
no validate source-mac
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

ND Inspection Policy Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Когда коммутатор получит ND-сообщение, содержащее адрес Link Layer, исходный MAC-адрес будет проверен на соответствие данному адресу Link Layer. При несовпадении адреса Link Layer и MAC- адреса пакет будет отброшен.

Пример

В данном примере показано, как настроить на коммутаторе действие отбрасывания для ND- сообщения, адрес Link Layer которого не соответствует MAC-адресу.

```
Switch# configure terminal
Switch(config)# ipv6 nd inspection policy policy1
Switch(config-nd-inspection)# validate source-mac
Switch(config-nd-inspection)#
```

58-3 device-role

Данная команда используется для указания роли подключенного устройства. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
device-role {host | router}
no device-role
```

Параметры

host	Укажите, чтобы настроить устройство в качестве узла (Host).
router	Укажите, чтобы настроить устройство в качестве маршрутизатора (Router).

По умолчанию

Роль устройства по умолчанию – Host.

Режим ввода команды

ND Inspection Policy Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать роль подключенного устройства. Так как по умолчанию устройство выполняет роль узла (Host), проверка сообщений NS и NA выполняется. Если устройство настроено в качестве маршрутизатора (Router), проверка сообщений NS и NA не выполняется. Сообщения NS и NA проверяются в соответствии с таблицей динамической привязки, информация о которой была получена из протокола ND или DHCP.

Пример

В данном примере показано, как создать политику ND под именем «policy1» и настроить устройство в качестве узла (Host).

```
Switch# configure terminal
Switch(config)# ipv6 nd inspection policy policy1
Switch(config-nd-inspection)# device-role host
Switch(config-nd-inspection)#
```

58-4 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки физического порта и port-channel. Используйте данную команду, чтобы применить политику ND Inspection Policy на определенном интерфейсе. Если указано **no policy-name**, для политики по умолчанию действуют следующие правила:

- Сообщения NS/NA проверяются.
- MAC-адрес источника в заголовке пакета уровня 2 не проверяется.

Пример

В данном примере показано, как применить политику ND Inspection Policy под именем «policy1» на интерфейсе Ethernet 1/0/3.

```
Switch# configure terminal
Switch(config)# ipv6 nd inspection policy policy1
Switch(config-nd-inspection)# device-role host
Switch(config-nd-inspection)# validate source-mac
Switch(config-nd-inspection)# exit
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ipv6 nd inspection attach-policy policy1
Switch(config-if)#
```

58-9 show ipv6 nd inspection policy

Данная команда используется для отображения информации о политике ND Inspection Policy.

show ipv6 nd inspection policy [*POLICY-NAME*]

Параметры

<i>POLICY-NAME</i>	(Опционально) Укажите имя политики ND Inspection Policy.
--------------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Если имя политики указано, отображаться будет информация только для указанной политики. Если имя политики не указано, отображаться будет информация для всех политик.

Пример

В данном примере показано, как отобразить конфигурацию политики под именем «inspect1» на всех интерфейсах, на которых применена данная политика.

```
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#
```


59. Команды Network Access Authentication

59-1 authentication guest-vlan

Данная команда используется для настройки Guest VLAN. При использовании формы **no** команда удалит Guest VLAN.

```
authentication guest-vlan VLAN-ID
no authentication guest-vlan
```

Параметры

VLAN-ID	Укажите Guest VLAN для аутентификации.
---------	--

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда не может быть использована, если указанная VLAN не существует в качестве статической VLAN. Узел не может получить доступ к сети, пока не пройдет аутентификацию. Если Guest VLAN настроена, узлу разрешается доступ только к Guest VLAN без прохождения аутентификации. Во время аутентификации, если RADIUS-сервер назначает пользователю VLAN, пользователь будет авторизован в назначенной VLAN. Назначение Guest VLAN и VLAN не действует на порт trunk VLAN и порт tunnel VLAN.

Обычно назначение Guest VLAN и VLAN действует для узлов, подключенных к нетегированным портам. Данный функционал не применим в случае, если узлы обмениваются тегированным трафиком.

Если режим узла (host mode) аутентификации настроен как multi-host, порт будет добавлен как Guest VLAN порт, а PVID порта будет изменен на Guest VLAN. Трафик, приходящий из Guest VLAN, будет перенаправлен независимо от аутентификации. Трафик, приходящий от других VLAN, будет отбрасываться, пока не пройдет аутентификацию. Когда один узел проходит аутентификацию, порт покидает Guest VLAN и будет добавлен в назначенную VLAN. PVID порта будет изменен на назначенную VLAN.

Если режим узла (host mode) аутентификации настроен как **multi-auth**, порт будет добавлен как Guest VLAN порт, и PVID порта будет изменен на Guest VLAN. Узлам, которым разрешен доступ к Guest VLAN, запрещен доступ к другим VLAN, пока они не пройдут аутентификацию. Когда один узел проходит аутентификацию, порт остается в Guest VLAN, а PVID порта не изменяется.

Если Guest VLAN отключена, порт выйдет из Guest VLAN и вернется к родной VLAN (native). PVID изменится на PVID родной VLAN.

Пример

В данном примере показано, как указать VLAN 5 в качестве Guest VLAN.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication guest-vlan 5
Switch(config-if)#
```

59-2 authentication host-mode

Данная команда используется для указания режима аутентификации. При использовании формы **no** команда вернется к значениям по умолчанию.

authentication host-mode {multi-host | multi-auth [vlan VLAN-ID [, | -]]}
no authentication host-mode [multi-auth vlan VLAN-ID [, | -]]

Параметры

multi-host	Укажите порт для работы в режиме multi-host. Выполняется только одна аутентификация, и все хосты, подключенные к порту будут разрешены.
multi-auth	Укажите порт для работы в режиме multi-auth. Каждый узел будет проходить аутентификацию индивидуально.
vlan VLAN-ID	(Опционально) Укажите VLAN аутентификации. Это может быть полезно, если различные VLAN на коммутаторе имеют различные требования к аутентификации. При использовании формы no все VLAN будут удалены, если не указаны конкретные. Это значит, что не важно, из какой VLAN клиент, клиент будет аутентифицирован, если MAC-адрес клиента (независимо от VLAN) не аутентифицирован. После аутентификации клиенту не нужно будет проходить повторную аутентификацию из других VLAN. Данная опция полезна для управления аутентификацией per-VLAN для портов trunk. Если режим аутентификации порта меняется на multi-host, предыдущие VLAN аутентификации на этом порту будут удалены.
,	(Опционально) Выделение серии или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию используется **multi-auth**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если порт работает в режиме **multi-host** и аутентифицирован один из узлов, всем другим узлам будет разрешен доступ к порту. Согласно аутентификации 802.1X, если повторная аутентификация завершается неудачно или аутентифицированный пользователь выходит из учетной записи, порт будет заблокирован на период молчания (quiet period). Порт восстановит обработку пакетов EAPOL после периода молчания.

Если порт работает в режиме **multi-auth**, каждый узел должен проходить аутентификацию индивидуально для доступа к порту. Узел представлен своим MAC-адресом. Доступ есть только у авторизованных узлов.

Пример

В данном примере показано, как назначить режим multi-host для порта Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication host-mode multi-host
Switch(config-if)#
```

59-3 authentication periodic

Данная команда используется для включения периодического повторения аутентификации для порта. При использовании формы **no** команда отключит периодическое повторение аутентификации.

authentication periodic
no authentication periodic

Параметры

Нет

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду для включения периодического повторения аутентификации для порта. Используйте команду **authentication timer reauthentication** для настройки таймера повторной аутентификации (re-authentication timer).

Пример

В данном примере показано, как включить периодическое повторение аутентификации для порта Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication periodic
Switch(config-if)#
```

59-4 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>	Укажите время, после которого неактивная сессия будет завершена. Доступен диапазон значений от 120 до 65535.
----------------	--

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если таймер бездействия настроен, сессия пользователя будет завершена, если сеанс не будет работать в течение настроенного периода времени. Таймер бездействия (inactivity timer) должен быть меньше, чем значение таймера, настроенного с помощью команды **authentication timer reauthentication**.

Пример

В данном примере показано, как настроить значение таймера бездействия 240 для Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication timer inactivity 240
Switch(config-if)#
```

59-5 authentication timer reauthentication

Данная команда используется для настройки таймера, по истечении которого будет необходимо пройти повторную аутентификацию. При использовании формы **no** команда вернется к значениям по умолчанию.

```
authentication timer reauthentication {SECONDS}
```

no authentication timer reauthentication**Параметры**

<i>SECONDS</i>	Укажите время, после которого будет необходимо пройти повторную аутентификацию. Доступен диапазон значений от 1 до 65535.
----------------	---

По умолчанию

По умолчанию используется значение 3600 секунд.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для настройки таймера, по истечении которого будет необходимо пройти повторную аутентификацию. Используйте команду **authentication periodic** для того, чтобы определить, будет ли производиться повторная аутентификация.

Пример

В данном примере показано, как настроить значение таймера повторной аутентификации 200 для Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication timer reauthentication 200
Switch(config-if)#
```

59-6 authentication timer restart

Данная команда используется для настройки таймера, по истечении которого станет возможна повторная аутентификация после последней неудачной попытки. При использовании формы **no** команда вернется к значениям по умолчанию.

authentication timer restart *SECONDS*
no authentication timer restart

Параметры

<i>SECONDS</i>	Укажите время, по истечении которого станет возможна повторная аутентификация. Доступен диапазон значений от 1 до 65535.
----------------	--

По умолчанию

По умолчанию используется значение 60 секунд.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Коммутатор будет в режиме молчания (Quiet State) после неудачной попытки аутентификации до истечения времени таймера.

Пример

В данном примере показано, как настроить значение таймера повторной аутентификации 20 для Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication timer restart 20
Switch(config-if)#
```

59-7 authentication username

Данная команда используется для создания пользователя в локальной базе данных аутентификации. При использовании формы **no** команда удалит пользователя из локальной базы данных аутентификации.

authentication username *NAME* **password** [**0** | **7**] *PASSWORD* [**vlan** *VLAN-ID*]
no authentication username *NAME* [**vlan**]

Параметры

<i>NAME</i>	Укажите имя пользователя, состоящее не более чем из 32 символов.
0	(Опционально) Пароль в обычном текстовом виде. Если не указан ни 0, ни 7, по умолчанию паролем будет обычный текст.
7	(Опционально) Зашифрованный пароль. Если не указан ни 0, ни 7, по умолчанию паролем будет обычный текст.
password <i>PASSWORD</i>	Укажите, чтобы задать пароль для MAC-аутентификации. Если указан пароль в обычном текстовом виде, длина строки не может превышать 32 символа.
vlan <i>VLAN-ID</i>	(Опционально) Укажите, чтобы назначить VLAN.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Данная команда используется для настройки локальной базы данных для аутентификации пользователей.

Пример

В данном примере показано, как создать локальную учетную запись с именем пользователя user1 и паролем pass1.

```
Switch# configure terminal
Switch(config)# authentication username user1 password pass1
Switch(config)#
```

59-8 clear authentication sessions

Данная команда используется для удаления сессий аутентификации.

clear authentication sessions {mac | wac | dot1x | all | interface *INTERFACE-ID* [mac | wac [dot1x] | mac-address *MAC ADDRESS*}

Параметры

mac	Укажите для удаления всех MAC-сессий.
wac	Укажите для удаления всех WAC-сессий.
dot1x	Укажите для удаления всех сессий dot1x.
all	Укажите для удаления всех сессий.
interface <i>INTERFACE-ID</i>	Укажите для удаления сессий порта.
mac-address <i>MAC ADDRESS</i>	Укажите для удаления всех сессий определенного пользователя.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для удаления сессий аутентификации.

Пример

В данном примере показано, как удалить сессии аутентификации на Ethernet 1/0/1.

```
Switch# clear authentication sessions interface ethernet 1/0/1
Switch#
```

59-9 authentication username mac-format

Данная команда используется для настройки формата MAC-адреса, который будет использоваться при аутентификации через RADIUS-сервер в качестве имени пользователя. При использовании формы **no** команда вернется к значениям по умолчанию.

```
authentication username mac-format case {lowercase | uppercase} delimiter {hyphen | colon | dot | none} number {1 | 2 | 5}
no authentication username mac-format
```

Параметры

lowercase	При аутентификации RADIUS формат имени пользователя будет выглядеть следующим образом: aa-bb-cc-dd-ee-ff
uppercase	При аутентификации RADIUS формат имени пользователя будет выглядеть следующим образом: AA-BB-CC-DD-EE-FF
hyphen	Укажите, чтобы использовать «-» в качестве разделителя. Формат будет выглядеть следующим образом: AA-BB-CC-DD-EE-FF
colon	Укажите, чтобы использовать «:» в качестве разделителя. Формат будет выглядеть следующим образом: AA:BB:CC:DD:EE:FF
dot	Укажите, чтобы использовать «.» в качестве разделителя. Формат будет выглядеть следующим образом: AA.BB.CC.DD.EE.FF
none	Укажите, чтобы не использовать знак разделения. Формат будет выглядеть следующим образом: AABCCDDEEFF
number	Укажите количество знаков разделения. Доступны следующие опции: 1: один разделитель; формат: AABCC.DDEEFF 2: два разделителя; формат: AAB.CCDD.EEFF 5: пять разделителей; формат: AA.BB.CC.DD.EE.FF Если выбран параметр none, знаки разделения ограничителей не будут использоваться.

По умолчанию

По умолчанию для MAC-адреса аутентификации используются большие буквы.
 По умолчанию знаком разделения MAC-адреса аутентификации является точка.
 По умолчанию используется два знака разделения MAC-адреса аутентификации.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для настройки формата имени пользователя на основе MAC-адреса, используемого при аутентификации RADIUS или для IGMP Security.

Пример

В данном примере показано, как настроить формат имени пользователя на основе MAC-адреса.

```
Switch# configure terminal
Switch(config)# authentication username mac-format case uppercase delimiter hyphen number 5
Switch(config)#
```

59-10 authentication compauth mode

Данная команда используется для указания режима Compound Authentication Mode. При использовании формы **no** команда вернется к значениям по умолчанию.

authentication compauth mode {any | mac-wac}
no authentication compauth mode

Параметры

any	Укажите для допуска, если допущен любой из методов аутентификации (802.1X, MAC-based Access Control и WAC). Если данный параметр используется, но MAC-based Access Control отключено, а 802.1X включено, то все равно будет необходима аутентификация 802.1X.
mac-wac	Укажите, чтобы сначала проводилась проверка MAC-based Access Control. Если клиент прошел аутентификацию MAC, WAC будет допущен. Оба метода аутентификации должны быть пройдены, чтобы аутентификация считалась успешной. Если используется данный параметр, доступ будет гарантирован после того, как два метода аутентификации будут успешно пройдены. Если один из методов аутентификации не был пройден, в доступе будет отказано. Если состояние аутентификации на порту или глобально включено, в доступе также будет отказано. После аутентификации информация об авторизации будет использоваться из модуля WAC.

По умолчанию

По умолчанию используется опция **any**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить или отключить методы аутентификации на физических портах.

Пример

В данном примере показано, как настроить режим mac-wac для Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#authentication comauth mode mac-wac
Switch(config-if)#
```

59-11 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>	Укажите, чтобы задать максимальное количество аутентифицированных пользователей. Доступен диапазон значений от 1 до 4096.
---------------	---

По умолчанию

По умолчанию ограничений нет.

Режим ввода команды

Global Configuration Mode Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда может использоваться в режиме Global Configuration Mode и Interface Configuration Mode.

Если команда настроена в режиме Global Configuration Mode, задается ограничение максимального количества пользователей на всю систему.

Если команда настроена в режиме Interface Configuration Mode, задается ограничение максимального количества пользователей на интерфейс.

Максимальное число пользователей включает пользователей 802.1X, MAC-based Access Control и WAC.

Также команда имеет следующее ограничение:

- Если новое число максимального количества пользователей меньше, чем текущее количество пользователей, команда будет отклонена, и появится сообщение об ошибке.

Пример

В данном примере показано, как назначить максимальное количество аутентифицированных пользователей для системы.

```
Switch# configure terminal
Switch(config)# authentication max users 256
Switch(config)#
```

59-12 authorization disable

Данная команда используется для отключения приема авторизованной конфигурации. При использовании формы **no** команда включит принятие авторизованной конфигурации.

```
authorization disable
no authorization disable
```

Параметры

Нет

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для включения или отключения принятия авторизованной конфигурации. Если авторизация включена для аутентификации, авторизованные атрибуты (например, VLAN, приоритет 802.1p по умолчанию, Bandwidth (полоса пропускания) и ACL (список управления доступом), назначенные RADIUS-сервером, будут приняты, если включено состояние авторизации. Bandwidth (полоса пропускания) и ACL (список управления доступом) назначаются на основе порта. В режиме multi-auth VLAN и 802.1p назначаются на основе узла.

Пример

В данном примере показано, как отключить состояние авторизации.

```
Switch# configure terminal
Switch(config)# no authorization disable
Switch(config)#
```

59-13 show authentication sessions

Данная команда используется для просмотра информации об аутентификации.

show authentication sessions [**mac** | **wac** | **dot1x** | **interface** *INTERFACE-ID* [, | -] [**mac** | **wac** | **dot1x**] | **mac-address** *MAC-ADDRESS*]

Параметры

mac	(Опционально) Укажите для отображения всех MAC-сессий.
wac	(Опционально) Укажите для отображения всех WAC-сессий.
dot1x	(Опционально) Укажите для отображения всех сессий dot1x.
interface <i>INTERFACE-ID</i>	(Опционально) Укажите порт для отображения.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
mac-address <i>MAC-ADDRESS</i>	(Опционально) Укажите для отображения определенного пользователя.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте команду без параметров, чтобы включить отображение сессий со всех портов.

Пример

В данном примере показано, как включить отображение сессий на Ethernet 1/0/1.

```

Switch# show authentication sessions interface ethernet 1/0/1

Interface: eth1/0/1
MAC Address: 00-16-76-35-1A-38
Authentication VLAN: 1
Authentication State: Success
Accounting Session ID: 0000000000CB
Authentication Username: wac
Client IP Address: 10.90.90.9
Aging Time: 3590 sec
Method   State
  WEB-based Access Control: Success, Selected

Total Authenticating Hosts: 0
Total Authenticated Hosts: 1
Total Blocked Hosts: 0

Switch#

```

Отображаемые параметры

Interface	Принимающий интерфейс узла аутентификации.
MAC Address	MAC-адрес узла аутентификации.
Authentication VLAN	Исходная VLAN начала аутентификации узла.
Authentication State	Состояние аутентификации узла. Start – принимается узел, но не было начала аутентификации Initialization – источник аутентификации готов, но новая аутентификация не начинается Authenticating – узел проходит аутентификацию Failure – ошибка аутентификации Success – узел прошел аутентификацию
Accounting Session ID	ID сессии учетной записи, который использовался для учета после аутентификации.
Authentication Username	Имя пользователя узла. Недоступно, пока узел выбран для MAC-Auth.
Client IP Address	Адрес ассоциированных клиентов. Доступен, только если узел выбран для Web-Auth.
Assigned VID	Назначенный VLAN ID, разрешенный после прохождения узлом аутентификации.
Assigned Priority	Назначенный приоритет, разрешенный после прохождения узлом аутентификации.
Assigned Ingress Bandwidth	Назначенный вход, разрешенный после прохождения узлом аутентификации.
Assigned Egress Bandwidth	Назначенный выход, разрешенный после прохождения узлом аутентификации.
Method	Метод аутентификации, например, 802.1X, MAC-Auth, Web-Auth и т.д.
State	Состояние метода аутентификации. Authenticating – узел проходит аутентификацию с

	<p>помощью данного метода</p> <p>Success – узел прошел аутентификацию с помощью данного метода аутентификации</p> <p>Selected – результат аутентификации данного метода, берется и анализируется системой для узла</p> <p>Failure – узел не прошел аутентификацию с помощью данного метода</p> <p>No Information – информация об аутентификации недоступна.</p>
Aging Time/Block Time	<p>Aging Time – время старения, период времени, во время которого аутентифицированный узел будет сохраняться в аутентифицированном состоянии. По истечении данного времени узел будет возвращен в неаутентифицированное состояние.</p> <p>Blocked Time – если узел не смог пройти аутентификацию, следующая попытка не начнется, пока не истечет время блокировки, если только пользователь не очистит состояние ввода entry state вручную.</p>
Idle Time	<p>Оставшееся время сессии аутентификации, которое будет завершено, если сессия неактивна в течение настроенного периода времени.</p> <p>Доступно только для сессий WEB.</p>
802.1X Authenticator State	<p>Состояние аутентификатора PAE 802.1X: возможны следующие значения:</p> <p>INITIALIZE – аутентификатор в процессе инициализации и ожидает запросы на аутентификацию.</p> <p>DISCONNECTED – инициализация завершена, но ни одно запрашивающее устройство не подключено к порту.</p> <p>CONNECTING – коммутатор обнаружил, что запрашивающее устройство подключается к порту. PAE произведет попытку подключиться к запрашивающему устройству.</p> <p>AUTHENTICATING – запрашивающее устройство проходит аутентификацию.</p> <p>AUTHENTICATED – аутентификатор успешно аутентифицировал запрашивающее устройство.</p> <p>ABORTING – процедура аутентификации преждевременно отменена из-за запроса на повторную авторизацию или запроса кадра EAPOL- Start, EAPOL-Logoff, тайм-аута аутентификации.</p> <p>HELD – коммутатор игнорирует или отбрасывает все EAPOL-пакеты для защиты от атак. В данное состояние можно перейти из состояния AUTHENTICATING после ошибки аутентификации.</p> <p>FORCE_AUTH – запрашивающее устройство всегда авторизовано</p> <p>FORCE_UNAUTH – запрашивающее устройство всегда не авторизовано.</p>
802.1X Backend State	<p>Состояние Backend PAE 802.1X. Возможны следующие значения:</p> <p>REQUEST – коммутатор получил пакет EAP-запроса от</p>

сервера аутентификации и отправил пакет запрашивающему устройству в качестве EAPOL-инкапсулированного кадра.

RESPONSE – коммутатор получил EAPOL-инкапсулированный пакет EAP-ответа от запрашивающего устройства и отправил EAP-пакет серверу аутентификации.

SUCCESS – сервер аутентификации подтвердил, что запрашивающее устройство является допустимым клиентом. Backend уведомит аутентификатор RAE и запрашивающее устройство.

FAIL – сервер аутентификации подтвердил, что запрашивающее устройство является недопустимым клиентом. Backend уведомит конечный автомат аутентификатор RAE и запрашивающее устройство.

TIMEOUT – на сервере аутентификации или запрашивающем устройстве есть тайм-аут.

IDLE – коммутатор ожидает начала новой сессии аутентификации.

INITIALIZE – аутентификатор производит инициализацию.

60. Команды Network Load Balancing (NLB)

60-1 nlb unicast-fdb

Данная команда используется для добавления одноадресной (unicast) NLB-записи в таблицу MAC-адресов (FDB). Используйте форму **no**, чтобы удалить одноадресную (unicast) NLB-запись из таблицы MAC-адресов (FDB) или удалить интерфейсы из NLB-записи.

```
nlb unicast-fdb MAC-ADDR interface INTERFACE-ID [, | -]
no nlb unicast-fdb MAC-ADDR [interface INTERFACE-ID [, | -]]
```

Параметры

<i>MAC-ADDR</i>	Укажите MAC-адрес записи создаваемой одноадресной NLB-записи. Адрес должен быть индивидуальным (unicast). Полученный пакет, MAC-адрес назначения которого соответствует указанному MAC-адресу, будет перенаправлен на указанный интерфейс.
interface <i>INTERFACE-ID</i>	Укажите интерфейс, на который будут перенаправлены соответствующие пакеты. Допустимыми интерфейсами являются физические порты.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы создать NLB-запись в таблицу unicast MAC-адресов. Функция Network Load Balancing (NLB) используется для поддержки Microsoft NLB, где у нескольких серверов может быть один и тот же IP-адрес и MAC-адрес. Запросы от клиентов будут отправлены на все серверы, но обработаны только одним из них. Существует два различных режима работы сервера:

- **Unicast Mode:** клиент для доступа к серверу в качестве MAC-адреса назначения использует индивидуальный MAC-адрес (unicast).
- **Multicast Mode:** клиент для доступа к серверу в качестве MAC-адреса назначения использует групповой MAC-адрес (multicast).

Данный MAC-адрес назначения называется общим MAC-адресом. Однако сервер использует собственный MAC-адрес (а не общий MAC-адрес) в качестве MAC-адреса источника в ответном пакете. Другими словами, индивидуальный адрес NLB не является MAC-адресом источника в пакете.

Полученный пакет, MAC-адрес назначения которого соответствует настроенному индивидуальному MAC-адресу, будет перенаправлен на соответствующие настроенные порты, независимо от конфигурации членства VLAN.

Администратор не может настроить статический адрес таблицы MAC-адресов в качестве адреса NLB. Однако MAC-адрес, созданный в качестве MAC-адреса NLB-записи, может быть динамически изучен в таблице MAC-адресов 2 уровня. В данном случае NLB имеет более высокий приоритет, а динамически изученная запись FDB не применяется.

Пример

В данном примере показано, как добавить индивидуальный адрес NLB в таблицу MAC-адресов. Добавленный адрес – 00-F3-22-0A-12-F4. Указанные интерфейсы передачи – от Ethernet 1/0/1 до Ethernet 1/0/5.

```
Switch# configure terminal
Switch(config)# nlb unicast-fdb 00-F3-22-0A-12-F4 interface ethernet 1/0/1-5
Switch(config)#
```

60-2 nlb multicast-fdb

Данная команда используется для добавления NLB-записи в таблицу групповых адресов. Используйте форму **no**, чтобы удалить NLB-запись из таблицы групповых адресов или удалить интерфейсы из записи NLB multicast.

nlb multicast-fdb *MAC-ADDR* **vlan** *VLAN-ID* **interface** *INTERFACE-ID* [, | -]
no nlb multicast-fdb *MAC-ADDR* **vlan** *VLAN-ID* [**interface** *INTERFACE-ID* [, | -]]

Параметры

<i>MAC-ADDR</i>	Укажите групповой MAC-адрес записи. Полученный пакет, MAC-адрес назначения которого соответствует указанному MAC-адресу, будет перенаправлен на указанные интерфейсы.
vlan <i>VLAN-ID</i>	Укажите VLAN ID записи. Доступный диапазон значений: от 1 до 4094.
interface <i>INTERFACE-ID</i>	Укажите интерфейс, на который будут перенаправлены соответствующие пакеты. Допустимыми интерфейсами являются физические порты.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы создать групповую NLB-запись. Данный MAC-адрес назначения называется общим MAC-адресом. Однако сервер использует собственный MAC-адрес (а не общий MAC-адрес) в качестве MAC-адреса источника в ответном пакете. Другими словами, индивидуальный адрес NLB не является MAC-адресом источника в пакете.

Многоадресная NLB-запись и многоадресная FDB-запись являются взаимоисключающими.

Соответствующие групповые MAC-адреса IPv6 (33:33:xx:xx:xx:xx) и зарезервированные MAC-адреса IEEE (01:80:c2:00:00:xx) не могут быть заданы в качестве групповых MAC-адресов записи NLB.

Пример

В данном примере показано, как создать многоадресную NLB-запись. Добавленный адрес – 01-F3-22-0A-12-F4. Указанные интерфейсы передачи – от Ethernet 1/0/1 до Ethernet 1/0/5 на VLAN 1.

```
Switch# configure terminal
Switch(config)# nlb multicast-fdb 01-F3-22-0A-12-F4 vlan 1 interface ethernet 1/0/1-5
Switch(config)#
```

60-3 show nlb fdb

Данная команда используется для отображения настроенных NLB-записей.

```
show nlb fdb
```

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения настроенных NLB-записей unicast и multicast.

Пример

В данном примере показано, как отобразить настроенные NLB-записи unicast и multicast.

```
Switch#show nlb fdb

MAC Address      VLAN ID  Interface
-----
00-11-22-33-44-55  ----    eth 1/0/20

Total Entries :1

Switch#
```

61. Команды Network Time Protocol (NTP)

61-1 ntp access-group

Данная команда используется для управления службами NTP на коммутаторе. Используйте форму **no**, чтобы отменить управление доступом служб NTP.

```
ntp access-group {default | IP-ADDRESS [IP-MASK] | IPV6-ADDRESS | IPV6-ADDRESS / PREFIX-LENGTH}
[ignore] [nomodify] [noquery] [nopeer] [noserve] [notrust] [version]
no ntp access-group {default | IP-ADDRESS [IP-MASK] | IPV6-ADDRESS | IPV6-ADDRESS / PREFIX-
LENGTH}
```

Параметры

default	Укажите, чтобы использовать IPv4-адрес (0.0.0.0/0.0.0.0) или IPv6-адрес (::/::) address по умолчанию. У IP-адреса по умолчанию всегда самый низкий приоритет в списке.
<i>IP-ADDRESS</i>	Укажите IP-адрес узла или сети.
<i>IP-MASK</i>	(Опционально) Укажите маску IP-адреса.
<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес узла или сети.
<i>IPV6-ADDRESS / PREFIX-LENGTH</i>	(Опционально) Укажите длину префикса IPv6.
ignore	(Опционально) Укажите, чтобы запретить доступ всем пакетам, включая NTP Control Queries.
nomodify	(Опционально) Укажите, чтобы запретить доступ NTP Control Queries, которые пытаются изменить состояние сервера.
noquery	(Опционально) Укажите, чтобы запретить доступ всем NTP Control Queries.
nopeer	(Опционально) Укажите, чтобы запретить доступ пакетам, которые могут быть ассоциированы без аутентификации. Пакеты могут быть: Broadcast, Symmetric-active и Manycast. Обратите внимание, что данный параметр применяется только к пакетам, которые могут быть ассоциированы.
noserve	(Опционально) Укажите, чтобы запретить доступ всем пакетам, кроме NTP Control Queries.
notrust	(Опционально) Укажите, чтобы запретить доступ пакетам, которые не прошли криптографическую аутентификацию. Если команда ntp authenticate включена, аутентификация проводится для всех пакетов, которые могут запустить ассоциацию. Если команда ntp authenticate отключена, но не присутствует параметр notrust , ассоциация может быть запущена независимо от того, аутентифицирован пакет или нет. Если команда ntp authenticate отключена, но параметр notrust указан, аутентификация требуется только для указанного диапазона адресов/масок.
version	(Опционально) Укажите, чтобы запретить доступ пакетам, не соответствующим текущей NTP-версии.

По умолчанию

По умолчанию все системы получают полный доступ, если указан только один параметр – **default**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

NTP реализует общее назначение списка управления доступом ACL (Access Control List), содержащего записи адресов/совпадений. Записи отсортированы по возрастанию значений адресов, а затем по возрастанию значений масок. Совпадение происходит, когда побитовое И (AND) маски и адреса источника пакета равно побитовому И (AND) маски и адреса в списке. Список просматривается по порядку и применяется политика последнего совпавшего правила.

Пример

В данном примере показано, как запретить новые ассоциации по умолчанию, кроме 192.43.244.18, 128.175.0.0/16 и 128.4.1.0/24, для которых требуется аутентификация.

```
Switch#configure terminal
Switch(config)#ntp access-group default nopeer
Switch(config)#ntp access-group 128.175.0.0 mask 255.255.0.0
Switch(config)#ntp access-group 128.4.1.0 mask 255.255.255.0 notrust
Switch(config)#ntp access-group 192.43.244.18
Switch(config)#
```

61-2 ntp authenticate

Данная команда используется для включения NTP-аутентификации. Используйте форму **no**, чтобы отключить NTP-аутентификацию.

```
ntp authenticate
no ntp authenticate
```

Параметры

Нет

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если NTP-аутентификация включена, сетевые узлы будут синхронизированы с коммутатором только при наличии ключа, указанного в команде **ntp trusted-key**.

Пример

В данном примере показано, как включить NTP-аутентификацию.

```
Switch# configure terminal
Switch(config)# ntp authenticate
Switch(config)#
```

61-3 ntp authentication-key

Данная команда используется для добавления ключа аутентификации для NTP. Используйте форму **no**, чтобы удалить ключ.

```
ntp authentication-key KEY-ID md5 VALUE
no ntp authentication-key KEY-ID
```

Параметры

<i>KEY-ID</i>	Укажите ID NTP-ключа. Доступный диапазон значений: от 1 до 255.
md5	Укажите тип MD5 для ключа аутентификации.
<i>VALUE</i>	Укажите ключевую строку. Максимально допустимое количество символов в строке – 32.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для добавления ключа аутентификации для NTP. Используйте форму **no**, чтобы удалить ключ.

Пример

В данном примере показано, как добавить ключ аутентификации. ID добавленного ключа – 45. Ключевая строка – NTPKey.

```
Switch#configure terminal
Switch(config)#ntp authentication-key 45 md5 NTPKey
Switch(config)#
```

61-4 ntp control-key

Данная команда используется для указания ID ключа для контрольных NTP-сообщений. Используйте форму **no**, чтобы удалить ключ.

```
ntp control-key KEY-ID
no ntp control-key
```

Параметры

<i>KEY-ID</i>	Укажите ID NTP-ключа. Доступный диапазон значений: от 1 до 255.
---------------	---

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для указания ID ключа для контрольных NTP-сообщений.

Пример

В данном примере показано, как указать ID ключа для контрольных NTP-сообщений.

```
Switch#configure terminal
Switch(config)#ntp control-key 45
Switch(config)#
```

61-5 ntp disable

Данная команда используется для отключения отправки NTP-пакетов на интерфейсе. Используйте форму **no**, чтобы включить от отправку NTP-пакетов на интерфейсе.

```
ntp disable
no ntp disable
```

Параметры

Нет

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для отключения/включения отправки NTP-пакетов на интерфейсе.

Пример

В данном примере показано, как отключить отправку NTP-пакетов на интерфейсе VLAN 1.

```
Switch# configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ntp disable
Switch(config-if)#
```

61-6 ntp master

Данная команда используется для настройки RTC в качестве основных NTP-часов, в случае если внешний NTP недоступен. Используйте форму **no**, чтобы отключить данную функцию.

```
ntp master STRATUM
no ntp master
```

Параметры

<i>STRATUM</i>	Укажите часовой слей NTP. Доступный диапазон значений: от 1 до 15.
----------------	--

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки RTC в качестве основных NTP-часов, в случае если внешний NTP недоступен. Используйте форму **no**, чтобы отключить данную функцию.

Пример

В данном примере показано, как настроить маршрутизатор в качестве основных часов NTP.

```
Switch#configure terminal
Switch(config)#ntp master 10
Switch(config)#
```

61-7 ntp max-associations

Данная команда используется для настройки максимального количества NTP-узлов и клиентов на коммутаторе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ntp max-associations NUMBER
no ntp max-associations
```

Параметры

<i>NUMBER</i>	Укажите количество NTP-ассоциаций. Доступный диапазон значений: от 1 до 64.
---------------	---

По умолчанию

Значение по умолчанию – 32.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки максимального количества NTP-узлов и клиентов на коммутаторе.

Пример

В данном примере показано, как настроить максимальное количество NTP-ассоциаций, равное 20.

```
Switch#configure terminal
Switch(config)#ntp max-associations 20
Switch(config)#
```

61-8 ntp peer

Данная команда используется для настройки NTP-узлов. Используйте форму **no**, чтобы отключить данную функцию.

```
ntp peer {IP-ADDRESS | IPv6-ADDRESS} [version NUMBER] [key KEY-ID] [prefer] [min-poll INTERVAL]
[max-poll INTERVAL]
no ntp peer {IP-ADDRESS | IPv6-ADDRESS}
```

Параметры

<i>IP-ADDRESS</i>	Укажите IPv4-адрес узла.
<i>IPv6-ADDRESS</i>	Укажите IPv6-адрес узла.
version	(Опционально) Укажите номер NTP-версии.
<i>NUMBER</i>	(Опционально) Введите номер NTP-версии. Доступный диапазон значений: от 1 до 4. Значение по умолчанию – 4.
key	(Опционально) Укажите ключ аутентификации.
<i>KEY-ID</i>	(Опционально) Укажите ID ключа аутентификации. Доступный диапазон значений: от 1 до 255.
prefer	(Опционально) Укажите предпочтительный для синхронизации узел.
min-poll	(Опционально) Укажите минимальный интервал опроса для NTP-сообщений. Интервал опроса рассчитывается как 2 в степени указанного значения. Например, если указано значение 6, то минимальный интервал опроса будет составлять 64 секунды ($2^6=64$).
<i>INTERVAL</i>	(Опционально) Укажите значение минимального интервала опроса. Значение по умолчанию – 6.
max-poll	(Опционально) Укажите максимальный интервал опроса для NTP-сообщений. Интервал опроса рассчитывается как 2 в степени указанного значения. Например, если указано значение 6, то максимальный интервал опроса будет составлять 64 секунды ($2^6=64$).
<i>INTERVAL</i>	(Опционально) Укажите значение максимального интервала опроса. Значение по умолчанию – 10.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Настройки NTP системного времени коммутатора могут быть синхронизированы с узлом.

Пример

В данном примере показано, как настроить IP-адрес 192.168.22.33 для NTP-узла с использованием NTP-версии 3.

```
Switch#configure terminal
Switch(config)#ntp peer 192.168.22.33 version 3
Switch(config)#
```

61-9 ntp request-key

Данная команда используется для указания ID ключа для NTP-пакетов Mode 7, используемых утилитой *ntpd*. Используйте форму **no**, чтобы удалить ключ.

```
ntp request-key KEY-ID
no ntp request-key
```

Параметры

<i>KEY-ID</i>	Укажите ID NTP-ключа. Доступный диапазон значений: от 1 до 255.
---------------	---

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Утилита *ntpd* использует проприетарный протокол (Proprietary Protocol), указанный для реализации NTP.

Пример

В данном примере показано, как указать ключ NTP Request.

```
Switch#configure terminal
Switch(config)#ntp request-key 45
Switch(config)#
```

61-10 ntp server

Данная команда используется для синхронизации времени коммутатора с NTP-сервером. Используйте форму **no**, чтобы отключить данную функцию.

```
ntp server {IP-ADDRESS | IPv6-ADDRESS} [version NUMBER] [key KEY-ID] [prefer] [min-poll INTERVAL]
[max-poll INTERVAL]
no ntp server {IP-ADDRESS | IPv6-ADDRESS}
```

Параметры

<i>IP-ADDRESS</i>	Укажите IPv4-адрес узла.
-------------------	--------------------------

<i>IPv6-ADDRESS</i>	Укажите IPv6-адрес узла.
version	(Опционально) Укажите номер NTP-версии.
<i>NUMBER</i>	(Опционально) Введите номер NTP-версии. Доступный диапазон значений: от 1 до 4. Значение по умолчанию – 4.
key	(Опционально) Укажите ключ аутентификации.
<i>KEY-ID</i>	(Опционально) Укажите ID ключа аутентификации. Доступный диапазон значений: от 1 до 255.
prefer	(Опционально) Укажите предпочтительный для синхронизации узел.
min-poll	(Опционально) Укажите минимальный интервал опроса для NTP- сообщений. Интервал опроса рассчитывается как 2 в степени указанного значения. Например, если указано значение 6, то минимальный интервал опроса будет составлять 64 секунды ($2^6=64$).
<i>INTERVAL</i>	(Опционально) Укажите значение минимального интервала опроса. Значение по умолчанию – 6.
max-poll	(Опционально) Укажите максимальный интервал опроса для NTP- сообщений. Интервал опроса рассчитывается как 2 в степени указанного значения. Например, если указано значение 6, то максимальный интервал опроса будет составлять 64 секунды ($2^6=64$).
<i>INTERVAL</i>	(Опционально) Укажите значение максимального интервала опроса. Значение по умолчанию – 10.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для синхронизации времени коммутатора с NTP-сервером.

Пример

В данном примере показано, как настроить IP-адрес 192.168.10.33 для NTP-сервера с использованием NTP-версии 2.

```
Switch#configure terminal
Switch(config)#ntp server 192.168.10.33 version 2
Switch(config)#
```

61-11 ntp trusted-key

Данная команда используется для указания доверенного ключа узла, который будет аутентифицирован NTP-системой. Используйте форму **no**, чтобы отключить данную функцию.

```
ntp trusted-key KEY-ID
no ntp trusted-key KEY-ID
```

Параметры

KEY-ID	Укажите ID NTP-ключа. Доступный диапазон значений: от 1 до 255.
--------	---

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для указания доверенного ключа узла, который будет аутентифицирован NTP-системой. Используйте форму **no**, чтобы отключить данную функцию.

Пример

В данном примере показано, как настроить доверенный NTP-ключ.

```
Switch#configure terminal
Switch(config)#ntp trusted-key 45
Switch(config)#
```

61-12 ntp update-calendar

Данная команда используется для периодической синхронизации аппаратных часов со временем, полученным по NTP. Используйте форму **no**, чтобы отключить данную функцию.

```
ntp update-calendar
no ntp update-calendar
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для периодической синхронизации аппаратных часов со временем, полученным по NTP. Используйте форму **no**, чтобы отключить данную функцию.

Пример

В данном примере показано, как периодически синхронизировать аппаратные часы со временем, полученным по NTP.

```
Switch#configure terminal
Switch(config)#ntp update-calendar
Switch(config)#
```

61-13 service ntp

Данная команда используется для включения NTP. Используйте форму **no**, чтобы отключить данную функцию.

service ntp
no service ntp

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки общего состояния NTP.

Пример

В данном примере показано, как включить NTP.

```
Switch#configure terminal
Switch(config)#service ntp
Switch(config)#
```

61-14 show ntp associations

Данная команда используется для отображения статуса NTP-ассоциаций.

show ntp associations [detail]

Параметры

detail	(Опционально) Укажите для отображения подробной информации по каждой NTP-ассоциации.
---------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения статуса NTP-ассоциаций.

Пример

В данном примере показано, как отобразить NTP-ассоциации.

```
Switch#show ntp associations

  Remote           Local           St Poll Reach  Delay  Offset  Disp
-----
-192.168.10.33    0.0.0.0         16 128   0 0.00000 0.000000 3.99217
+192.168.22.33   0.0.0.0         16 128   0 0.00000 0.000000 3.99217
+ Symmetric active, - Symmetric passive, = Client, * System Peer

Switch#
```

Отображаемые параметры

Leading Characters	Нижне перечислены возможные первые символы в строке, отображаемой на дисплее: + – Symmetric Active Mode - – Symmetric Passive Mode = – Client Mode ^ – Broadcast Mode
---------------------------	---

	~ – Broadcast Client * – System Peer
Remote	IP-адрес узла.
Local	IP-адрес локального интерфейса.
St	Часовой слой узла.
Poll	Интервал опроса в секундах.
Reach	Успешное достижение узла.
Delay	Задержка прохождения сигнала в прямом и обратном направлении к одноранговому узлу.
Offset	Относительное время узла по отношению к локальному времени в миллисекундах. (Положительное значение указывает, что показания часов сервера больше. Отрицательное значение указывает, что показания часов узла больше).
Disp	Дисперсия (Dispersion). Максимальная разница во времени, которая когда-либо наблюдалась между локальными часами и часами сервера.

В данном примере показано, как отобразить NTP-ассоциации подробно.

```
Switch# show ntp associations detail

Remote 192.168.10.33, Local 0.0.0.0
Our mode client, Peer mode unspec, Stratum 16, Precision -7
Leap 11, RefID [INIT], RootDistance 0.00000, RootDispersion 0.00000
PPoll 10, HPoll 10, KeyID 0, Version 2, Association 8356
Reach 000, Unreach 17, Flash 0x1400, Timer 840s, flags Config
Reference Timestamp: 00000000.00000000 Thu, Feb 7 2036 6:28:16.00000
Originate Timestamp: 00000000.00000000 Thu, Feb 7 2036 6:28:16.00000
Receive Timestamp: 00000000.00000000 Thu, Feb 7 2036 6:28:16.00000
Transmit Timestamp: 00000000.00000000 Thu, Feb 7 2036 6:28:16.00000
Filter Delay: 0.00000 0.00000 0.00000 0.00000
              0.00000 0.00000 0.00000 0.00000
Filter Offset: 0.000000 0.000000 0.000000 0.000000
              0.000000 0.000000 0.000000 0.000000
Filter Order: 0      1      2      3
              4      5      6      7
Offset 0.000000, Delay 0.00000, Error Bound 3.99217, Filter Error 0.00000

Remote 192.168.22.33, Local 0.0.0.0
Our mode sym_active, Peer mode unspec, Stratum 16, Precision -7
Leap 11, RefID [INIT], RootDistance 0.00000, RootDispersion 0.00000
PPoll 10, HPoll 10, KeyID 0, Version 3, Association 8355
Reach 000, Unreach 17, Flash 0x1400, Timer 798s, flags Config
Reference Timestamp: 00000000.00000000 Thu, Feb 7 2036 6:28:16.00000
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Отображаемые параметры

Remote	IP-адрес узла.
Local	IP-адрес коммутатора.

Our mode	Наш режим по отношению к узлу. Доступные режимы: active, passive, client, server, bdcast и bdcastclient .
Peer mode	Режим узла по отношению к нам.
Stratum	Часовой слой узла.
Precision	Точность часов узла в Гц.
Leap	Leap-индикатор. Доступный диапазон значений: от 0 до 3.
RefID	IP-адрес узла устройства, с которым необходимо настроить синхронизацию.
RootDistance	Корневая задержка. Задержка в миллисекундах к корневому устройству настройки NTP.
RootDispersion	Корневая дисперсия. Максимальная разница во времени, которая когда-либо наблюдалась между локальными и корневыми часами.
PPoll	Экспонента опроса узла (Peer).
HPoll	Экспонента опроса хоста (Host).
KeyID	ID ключа аутентификации.
Version	NTP-версия, используемая узлом.
Association	ID ассоциации.
Reach	Успешное достижение узла.
Unreach	Счетчик неуспешных попыток достижения узла.
Flash	Необходима диагностика для выявления проблем.
Timer	Таймер узла в секундах.
Flags	Флаги узла.
Reference Timestamp	Время последней установки или корректировки системных часов.
Originate Timestamp	Время отправленного запроса клиента на сервер.
Receive Timestamp	Время полученного запроса клиента на сервер.
Transmit Timestamp	Время отправленного ответа сервера клиенту.
Filter Delay	Задержка приема/передачи (Round-Trip Delay) каждой выборки в миллисекундах.
Filter Offset	Сдвиг часов (Clock Offset) каждой выборки в миллисекундах.
Filter Order	Порядок фильтрации каждой выборки.
Offset	Сдвиг часов узла по отношению к нашему времени.
Delay	Задержка приема/передачи (Round-Trip Delay) для узла.
Error Bound	Дисперсия (Dispersion) узла.
Filter Error	Ошибка аппроксимации (Approximate Error) каждой выборки.
St	Часовой слой узла.
Poll	Интервал опроса в секундах.
Reach	Успешное достижение узла.
Delay	Задержка прохождения сигнала в прямом и обратном направлении к одноранговому узлу.
Offset	Относительное время узла по отношению к локальному времени в миллисекундах. (Положительное значение указывает, что показания часов сервера больше.)

	Отрицательное значение указывает, что показания часов узла больше).
Disp	Дисперсия (Dispersion). Максимальная разница во времени, которая когда-либо наблюдалась между локальными часами и часами сервера.

61-15 show ntp status

Данная команда используется для отображения статуса функции NTP.

show ntp status

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения статуса функции NTP.

Пример

В данном примере показано, как отобразить статус функции NTP.

```
Switch# show ntp status

Leap Indicator:      Unsynchronized
Stratum:             16
Precision:           -8
Root Distance:       0.00000 s
Root Dispersion:     0.10680 s
Reference ID:        [INIT]
Reference Time:      00000000.00000000 Thu, Feb 7 2036 6:28:16.00000
System Flags:        Auth Monitor NTP Kernel Stats
Jitter:              0.000000 s
Stability:           0.000 ppm
Auth Delay:          0.000000 s

Switch#
```

Отображаемые параметры

Remote	IP-адрес узла.
Local	IP-адрес коммутатора.
Our mode	Наш режим по отношению к узлу. Доступные режимы: active, passive, client, server, bdcast и bdcastclient .
Peer mode	Режим узла по отношению к нам.
Leap Indicator	Synchronized – коммутатор синхронизирован с NTP-узлом. Unsynchronized – коммутатор не синхронизирован с NTP-узлом.
Stratum	Часовой слой коммутатора.
Precision	Точное значение.
RootDistance	Корневая задержка. Задержка в миллисекундах к корневому устройству настройки NTP.
RootDispersion	Корневая дисперсия. Максимальная разница во времени, которая когда-либо наблюдалась между локальными и корневыми часами.
Reference ID	IP-адрес узла устройства, с которым необходимо настроить синхронизацию.
Reference Time	Эталонная временная метка (Reference Timestamp).
System Flags	Auth – необходимо настроить аутентификацию. Monitor – включение монитора. NTP – функция NTP включена. Kernel – поддержка ядра включена. Stats – контроль статуса системы.
Jitter	Джиттер системы.
Stability	Стабильность частоты (Wander) (s/s).
Auth Delay	Задержка аутентификации.

62. Команды Power over Ethernet (PoE)

62-1 poe pd description

Данная команда используется для описания PD-устройства (питаемого устройства), подключенного к порту PoE. Используйте форму **no**, чтобы удалить описание.

```
poe pd description TEXT
no poe pd description
```

Параметры

<i>TEXT</i>	Укажите описание PD-устройства, подключенного к порту PoE. Максимально допустимое количество символов в строке – 32.
-------------	--

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать описание PD-устройства, подключенного к физическому порту.

Пример

В данном примере показано, как указать описание для PoE PD-устройства на интерфейсе Eth3/0/1.

```
Switch(config)# interface eth3/0/1
Switch(config-if)# poe pd description For VOIP usage
```

62-2 poe pd legacy-support

Данная команда используется для включения поддержки устаревших PD-устройств (legacy PD). Используйте форму **no**, чтобы отключить поддержку.

```
poe pd legacy-support
no poe pd legacy-support
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить поддержку устаревших PD-устройств (legacy PD), подключенных к физическому порту.

Пример

В данном примере показано, как включить поддержку для устаревших PD-устройств (legacy PD), подключенных к интерфейсу Eth3/0/1.

```
Switch(config)# interface eth3/0/1
Switch(config-if)# poe pd legacy-support
```

62-3 poe pd priority

Данная команда используется для настройки приоритета при подаче питания порту. Используйте форму **po**, чтобы вернуться к настройкам по умолчанию.

```
poe pd priority {critical | high | low}
no poe pd priority
```

Параметры

critical	Укажите, чтобы назначить наивысший приоритет PD-устройству, подключенному к порту.
high	Укажите, чтобы назначить высокий приоритет PD-устройству, подключенному к порту.
low	Укажите, чтобы назначить низкий приоритет PD-устройству, подключенному к порту.

По умолчанию

По умолчанию назначен низкий приоритет.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки физического порта.

Поскольку бюджет мощности ограничен, источника питания может быть недостаточно для подачи питания при добавлении к системе новых PD-устройств. В данном случае система PoE входит в критическую секцию. Подача питания новому добавленному PD-устройству будет зависеть от политики, настроенной в команде **poe policy preempt**.

Политика, для которой отключен режим Preempt, обслуживается в первую очередь. Таким образом, новое PD-устройство не будет обеспечено питанием.

При включенном режиме Preempt для политики PD-устройство с наименьшим приоритетом будет вытеснено новым подключенным PD-устройством с более высоким приоритетом.

Пример

В данном примере показано, как настроить наивысший приоритет на интерфейсе Eth 3/0/1.

```
Switch(config)# interface eth3/0/1
Switch(config-if)# poe pd priority critical
Switch(config-if)# end
Switch(config)#
```

62-4 poe policy preempt

Данная команда позволяет при недостаточном бюджете мощности отключать питание PD-устройства с наименьшим приоритетом для освобождения мощности для нового подключенного PD-устройства с более высоким приоритетом. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

poe unit *UNIT-ID* policy preempt
no poe unit *UNIT-ID* policy preempt

Параметры

<i>UNIT-ID</i>	(Опционально) Укажите Unit ID устройства, информацию о котором необходимо отобразить.
----------------	---

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Поскольку бюджет мощности ограничен, источника питания может быть недостаточно для подачи питания при добавлении к системе новых PD-устройств. В данном случае система PoE входит в критическую секцию.

Подача питания новому добавленному PD-устройству будет зависеть от политики, настроенной в данной команде. Политика, для которой отключен режим Preempt, обслуживается в первую очередь. Таким образом, новое PD-устройство не будет обеспечено питанием.

При включенном режиме Preempt для политики PD-устройство с наименьшим приоритетом будет вытеснено новым подключенным PD-устройством с более высоким приоритетом.

Пример

В данном примере показано, как настроить режим Preempt для политики обслуживания системной мощности PoE.

```
Switch(config)# poe policy preempt
```

62-5 poe power-inline

Данная команда используется для настройки режима Power Management Mode (управление энергопотреблением) для портов PoE. Используйте форму **no**, чтобы удалить привязку профиля временного диапазона или вернуться к настройкам по умолчанию.

```
poe power-inline {auto [max MAX-WATTAGE] [time-range PROFILE-NAME] | never}
no poe power-inline [auto {max | time-range}
```

Параметры

auto	Укажите, чтобы PD-устройства были обнаружены автоматически для подачи питания.
max MAX-WATTAGE	(Опционально) Укажите максимальную мощность питания для автоматически обнаруженного PD-устройства. Если не указано, максимальная мощность будет определена классом данного устройства. Доступный диапазон значений: от 1000 мВт до неограниченного значения.
time-range PROFILE-NAME	(Опционально) Укажите имя профиля временного диапазона для настройки периода активации.
never	Укажите, чтобы отключить питание PD-устройства, подключенного к порту.

По умолчанию

По умолчанию используется параметр **auto**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется только на портах с поддержкой PoE.

При использовании параметра **auto** PD-устройство будет обнаружено автоматически для подачи питания. В команде возможно указание максимальной мощности для порта. Если не указано, максимальная мощность

будет определена классом PD-устройства. PD-устройство не будет обеспечено питанием, если для его работы требуется мощность выше настроенной максимальной мощности.

Если к порту PoE привязан профиль временного диапазона, порт будет работать только в течение периода времени, указанного в профиле. Таким образом, PD-устройство будет обеспечено питанием только в указанный период времени.

Чтобы распределить бюджет мощности заранее, необходимо порт перевести в режим Static Mode. Бюджет мощности будет распределен на порт, даже если PD-устройство не подключено к порту. Если указана максимальная мощность, то указанное количество мощности выделяется заранее.

Настройка профиля временного диапазона является опциональной. Если профиль временного диапазона не указан, временной диапазон не назначается.

Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

Пример

В данном примере показано, как настроить автоматическое обнаружение PD-устройства для подачи питания на интерфейсе Eth3/0/1.

```
Switch(config)# interface range eth3/0/1
Switch(config-if)# poe power-inline auto
```

В данном примере показано, как настроить максимальную мощность на интерфейсе Eth3/0/1. Настроенная максимальная мощность позволяет подключиться PD-устройству, для работы которого требуется не более 5000 мВт.

```
Switch(config)# interface eth3/0/1
Switch(config-if)# poe power-inline auto 5000
```

В данном примере показано, как отключить обнаружение PD-устройства и прекратить подачу питания с интерфейса Eth3/0/1.

```
Switch(config)# interface eth3/0/1
Switch(config-if)# poe power-inline never
```

В данном примере показано, как привязать профиль временного диапазона «day_time» к интерфейсу Eth3/0/1.

```
Switch(config)# interface eth3/0/1
Switch(config-if)# poe power-inline auto time-range day_time
```

62-6 poe usage-threshold

Данная команда используется для настройки порога потребления для отправки уведомлений. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
poe unit UNIT-ID usage-threshold PERCENTAGE
no poe unit UNIT-ID usage-threshold
```

Параметры

<i>PERCENTAGE</i>	Укажите порог потребления для отправки уведомлений. Доступный диапазон значений: от 1 до 99. Единица измерения – проценты.
<i>UNIT-ID</i>	(Опционально) Укажите Unit ID устройства, информацию о котором необходимо отобразить.

По умолчанию

Значение по умолчанию – 99.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

При превышении PD-устройством настроенного порога потребления будет выслано trap-сообщение «pethMainPowerUsageOnNotification». Trap-сообщение «pethMainPowerUsageOffNotification» свидетельствует о том, что процентное значение порога стало меньше указанного.

Пример

В данном примере показано, как настроить порог потребления для уведомлений до 50%.

```
Switch(config)# poe unit 1 usage-threshold 50
Switch(config)#
```

62-7 snmp-server enable traps poe

Данная команда используется для включения отправки уведомлений о событиях PoE. Используйте форму **no**, чтобы отключить отставку уведомлений о событиях PoE.

```
snmp-server enable traps poe [unit UNIT-ID]
no snmp-server enable traps poe [unit UNIT-ID]
```

Параметры

<i>UNIT-ID</i>	(Опционально) Укажите Unit ID устройства, информацию о котором необходимо отобразить.
----------------	---

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить отправку trap-сообщений для PoE о превышении порога потребления.

Пример

В данном примере показано, как настроить отправку trap-сообщений о событии PoE.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps poe
Switch(config)#
```

62-8 clear poe statistic

Данная команда используется для обнуления счетчиков статистики на порту.

clear poe statistic {all | interface *INTERFACE-ID* [,|-]}

Параметры

all	Укажите, чтобы удалить статистику на всех интерфейсах.
interface <i>INTERFACE-ID</i>	Укажите ID интерфейса. Допустимыми интерфейсами являются физические порты.
,	(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

Privilege EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Для отображения счетчиков записей статистики используйте команду **show poe power-inline statistics**. Данная команда применяется для удаления всех значений счетчиков на порту.

Пример

В данном примере показано, как удалить статистику на интерфейсе Eth3/0/1.

```
Switch# clear poe statistic interface eth3/0/1
```

62-9 show poe power-inline

Данная команда используется для отображения статуса PoE для определенного порта PoE или для всех портов PoE в системе коммутатора.

```
show poe power-inline [INTERFACE-ID [, | -]] {status | configuration | statistics | measurement | lldp-classification}
```

Параметры

<i>INTERFACE-ID</i>	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.
status	Укажите для отображения статуса PoE порта.
configuration	Укажите для отображения информации о настройках порта.
statistics	Укажите для отображения счетчиков ошибок.
measurement	Укажите для отображения напряжения, тока, потребляемой мощности и температуры.
lldp-classification	Укажите для отображения классификации Data Link Layer, используя информацию о Power via MDI TLV.

По умолчанию

Нет

Режим ввода команды

EXEC Mode

Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить статус PoE порта, статус конфигурации Power Inline, счетчики статистики, результаты параметра **measurement** и классификацию Data Link Layer. Если ID интерфейса не указан, будут отображены все интерфейсы PoE. Отображаются только интерфейсы с поддержкой PoE.

Пример

В данном примере показан вывод команды **show poe power-inline status**.

```

Switch> show poe power-inline status
Interface  State      Class  Max(W)  Used(W)  Description
-----
eth3/0/1   delivering class-1 4      3.4     IP-camera-1
eth3/0/2   delivering class-2 10     6.3     12345678901234567890123456789012
!--- Output suppressed...
eth4/0/1   delivering class-3 15.4   13.0eth4/0/2   delivering class-3 15.4   12.4
eth4/0/3   disabled  n/a    0       0
eth4/0/4   searching n/a    11.0   0
!--- Output suppressed...
eth5/0/24  disabled  n/a    0       0
eth5/0/25  faulty[2]  n/a    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>

```

62-10 show poe power module

Данная команда используется для отображения настроек и фактических значений PD-устройств.

show poe power module [unit *UNIT-ID*] [detail]

Параметры

detail	(Опционально) Укажите для отображения более подробной информации о питании и параметров для PD-устройств.
<i>UNIT-ID</i>	(Опционально) Укажите Unit ID устройства, информацию о котором необходимо отобразить.

По умолчанию

Нет

Режим ввода команды

EXEC Mode

Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить подробную информацию о питании и параметры для PoE-устройств.

Пример

В данном примере показано, как отобразить информацию о питании PoE системы.

```
Switch> show poe power module
```

Unit	Delivered(W)	Power Budget (W)	Usage-Threshold(%)	Preempt	Trap State
2	14	300	99	Enabled	Enabled
3	740	750	99	Disabled	Enabled
4	115	600	80	Enabled	Enabled
5	0	200	75	Disabled	Disabled

```
Switch>
```

63. Команды Policy-Based Routing (PBR)

63-1 ip policy route-map

Данная команда используется для указания карты маршрута (Route-map) в качестве политики маршрутизации на интерфейсе. Используйте форму **no**, чтобы отключить политику маршрутизации на интерфейсе.

```
ip policy route-map MAP-NAME
no ip policy route-map
```

Параметры

<i>MAP-NAME</i>	Укажите имя карты маршрута (Route-map), которую необходимо использовать в качестве политики маршрутизации.
-----------------	--

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется только для настройки интерфейса VLAN.

Укажите одну карту маршрута (Route-map) в качестве политики маршрутизации на интерфейсе. Настроенная политика будет применена к пакетам, полученным на указанном интерфейсе.

Используйте команду **match ip-address**, чтобы настроить критерии соответствия для пакетов с определенными характеристиками. Если при вводе команды **match ip-address** используется список доступа IP, проверяются все критерии соответствия в данном списке доступа. Пакеты, прошедшие проверку на соответствие, будут обработаны на основе настроенной карты маршрута.

Маршрутизация пакетов, не соответствующих списку доступа, осуществляется на основе таблицы маршрутизации.

Ниже перечислены команды для применения необходимых действий, связанных с маршрутизацией на основе политики (Policy-Based Routing):

- **set ip precedence**
- **set ip next-hop**
- **set ip default next-hop**

Команды, перечисленные выше, не будут применены, если при указании карты маршрута использовалась команда **no match ip-address**, а также если настроенный список доступа IP не существует или не содержит правила. В данном случае политика не будет применена на интерфейсе.

Пример

В данном примере показано, как настроить политику маршрутизации для маршрутизации пакетов, соответствующих списку доступа IP «pbr-acl». Следующий узел (Next Hop) – 20.1.1.254.

```
Switch# configure terminal
Switch(config)# route-map pbr-map permit 1
Switch(config-route-map)# match ip address pbr-acl
Switch(config-route-map)# set ip next-hop 20.1.1.254
Switch(config-route-map)# exit
Switch(config)# interface vlan 100
Switch(config-if)# ip policy route-map pbr-map
Switch(config-if)#
```

63-2 show ip policy

Данная команда используется для отображения карты маршрута, используемой для маршрутизации на основе политики (Policy-Based Routing).

show ip policy

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию о маршрутизации на основе политики, настроенной на интерфейсах.

Пример

В данном примере показано, как отобразить информацию о маршрутизации на основе политики, настроенной на интерфейсах.

```
Switch#show ip policy
```

```
Interface    Route Map
```

```
-----  
vlan 1      pbr-map1
```

```
vlan 2      pbr-map2
```

```
vlan 100    pbr-map3
```

```
Total Entries: 3
```

```
Switch#
```


64. Команды Port Security

64-1 clear port-security

Данная команда позволяет удалить динамически изученные безопасные MAC-адреса.

```
clear port-security {all | {address MAC-ADDR | interface INTERFACE-ID [, | -]} [vlan VLAN-ID]}
```

Параметры

all	Укажите, чтобы удалить все динамически изученные безопасные MAC- адреса.
address MAC-ADDR	Укажите, чтобы удалить указанные динамически изученные безопасные записи на основе введенного MAC-адреса.
interface INTERFACE-ID	Укажите, чтобы удалить все динамически изученные безопасные записи на указанном интерфейсе.
,	(Опционально) Выделение серии интерфейсов или разделение группы интерфейсов от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.
vlan VLAN-ID	Укажите, чтобы удалить динамически изученные записи, информация о которых была получена через указанную VLAN.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда позволяет удалить автоматически изученные безопасные MAC-адреса, как динамические, так и постоянные.

Пример

В данном примере показано, как удалить определенный безопасный адрес из таблицы MAC-адресов.

```
Switch# clear port-security address 0080.0070.0007
Switch#
```

64-2 show port-security

Данная команда используется для просмотра текущих настроек Port Security.

show port-security [[interface *INTERFACE-ID* [, | -]] [address] | vlan *VLAN-ID* [, | -]]

Параметры

interface <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.
address	(Опционально) Укажите для отображения безопасных MAC-адресов, включая настроенные и изученные адреса.
vlan <i>VLAN-ID</i>	(Опционально) Укажите для отображения настроек Port Security для VLAN.
,	(Опционально) Выделение серии VLAN или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

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#
```

64-3 snmp-server enable traps port-security

Данная команда используется для включения отправки SNMP-уведомлений при обнаружении функционалом Port Security недопустимых адресов. При использовании формы **no** команда отключит отправку SNMP-уведомлений.

```
snmp-server enable traps port-security [trap-rate TRAP-RATE]
no snmp-server enable traps port-security [trap-rate]
```

Параметры

trap-rate <i>TRAP-RATE</i>	(Опционально) Укажите количество трапов в секунду. Доступен диапазон значений от 0 до 1000. Значение по умолчанию 31 означает, что SNMP trap будет генерироваться для каждого нарушения безопасности.
-----------------------------------	---

По умолчанию

По умолчанию функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для включения или отключения отправки SNMP-уведомлений при обнаружении функционалом Port Security недопустимых адресов.

Пример

В данном примере показано, как включить отправку трапов при обнаружении функционалом Port Security недопустимых адресов и установить количество трапов в секунду, равное 3.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps port-security
Switch(config)# snmp-server enable traps port-security trap-rate 3
Switch(config)#
```

64-4 switchport port-security

Данная команда используется для настройки параметров Port Security, чтобы ограничить количество пользователей, которым разрешен доступ к порту. Используйте форму **no** этой команды для отключения Port Security или удаления безопасного MAC-адреса.

```
switchport port-security [maximum VALUE | violation {protect | restrict | shutdown} | mode
{permanent | delete-on timeout} | mac-address [permanent] MAC-ADDRESS [vlan VLAN-ID]]
no switchport port-security [maximum | violation | mode | mac-address [permanent] MAC-ADDRESS
[vlan VLAN-ID]]
```

Параметры

maximum <i>VALUE</i>	(Опционально) Укажите максимальное число разрешенных безопасных MAC-адресов. Если не указано, значение по умолчанию – 32. Доступен диапазон значений от 0 до 12288
protect	(Опционально) Укажите, если необходимо отбрасывать все пакеты с незащищенных узлов на уровне port-security без возрастания счетчика нарушения безопасности (security-violation).
restrict	(Опционально) Укажите, если необходимо отбрасывать все пакеты с незащищенных узлов на уровне port-security, с возрастанием счетчика нарушения безопасности (security-violation) и записью в системный журнал (system log).
shutdown	(Опционально) Укажите для отключения порта, если произошло нарушение безопасности и для записи в системный журнал (system log).
permanent	(Опционально) В данном режиме все изученные MAC-адреса не будут удалены, пока пользователь не удалит их вручную.
delete-on timeout	(Опционально) В данном режиме все изученные MAC-адреса будут удалены, когда запись устареет, или если пользователь удалит записи вручную.
mac-address <i>MAC-ADDRESS</i>	(Опционально) Укажите, чтобы добавить безопасный MAC-адрес для получения доступа к порту.
permanent	(Опционально) Укажите, чтобы задать безопасный постоянно настроенный MAC-адрес порта. Данная запись является такой же, как изученная в режиме Permanent Mode.
vlan <i>VLAN-ID</i>	(Опционально) Укажите VLAN. Если VLAN не указана, MAC-адрес будет изучен в соответствии с PVID.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Когда включена функция Port Security, если режим порта port mode настроен как **delete-on-timeout**, порт автоматически будет изучать безопасные записи и хранить их, пока не истечет их время тайм-аута. Время хранения этих записей зависит от настроек, заданных командой **switchport port-security aging**. Если режим порта задан как постоянный (permanent), он будет автоматически изучать безопасные записи с неистекающим тайм-аутом. Автоматически изученные безопасные записи будут храниться в текущем файле конфигурации (running configuration).

При изменении состояния безопасности режима порта (port mode-security) счетчик нарушений будет сброшен, записи Auto-permanent будут преобразованы в соответствующие динамические записи. При отключении режима порта port-security автоматически изученные безопасные записи будут удалены, включая динамические и постоянные (Permanent), а также счетчик нарушений. При изменении настройки VLAN автоматически изученные динамические безопасные записи будут удалены.

Постоянные безопасные записи будут храниться в текущем файле конфигурации (running configuration) и могут быть сохранены в NVRAM при использовании команды **copy**. Настроенные пользователем безопасные MAC-адреса будут подсчитываться в максимальном количестве MAC-адресов на порт.

Так как постоянная (permanent) безопасная запись Port Security включена на порту, MAC-адрес нельзя перенести на другой порт.

При изменении настроек изученные адреса останутся неизменными, если максимальное число будет увеличено. Если максимальное число будет изменено на меньшее, чем существующее число изучаемых записей, команда будет отклонена.

Порт с поддержкой Port Security имеет следующие ограничения:

- Функция Port Security не может функционировать одновременно с 802.1X, MAC-based Access Control (управление доступом на основе MAC), WAC и IMPB, которые предоставляют более широкие возможности управления безопасностью.
- Если порт указан в качестве порта назначения для функции зеркалирования, функция Port Security не может быть включена.
- Если порт указан в качестве порта агрегирования каналов, функция Port Security не может быть включена.

При превышении максимального количества безопасных пользователей, может быть предпринято одно из следующих действий:

- **Protect** – когда число безопасных MAC-адресов порта достигает максимального значения пользователей, разрешенного на порту, пакеты с неизвестным адресом источника будут отбрасываться до тех пор, пока какая-нибудь безопасная запись не будет удалена.
- **Restrict** – при нарушении безопасности происходит ограничение данных, и возрастает счетчик нарушений безопасности.
- **Shutdown** – при нарушении безопасности интерфейс отключается на основе ошибок.

Пример

В данном примере показано, как настроить режим permanent для Port Security с 5 безопасными MAC-адресами, разрешенными на порту.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security mode permanent
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)#
```

В данном примере показано, как вручную добавить безопасный MAC-адрес 00-00-12-34-56-78 с VID 5 на Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security mac-address 00-00-12-34-56-78 vlan 5
Switch(config-if)#
```

В данном примере показано, как настроить отбрасывание всех пакетов от небезопасных узлов на уровне port-security с увеличением счетчика нарушений при обнаружении нарушений безопасности.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)#
```

64-5 switchport port-security aging

Данная команда позволяет задать время старения (aging time) для динамически изученных безопасных адресов на интерфейсе. При использовании формы **no** команда вернется к значениям по умолчанию.

```
switchport port-security aging {time MINUTES | type {absolute | inactivity}}
no switchport port-security aging {time | type}
```

Параметры

time <i>MINUTES</i>	Укажите время старения (aging time) для динамически изученных безопасных адресов на порту в минутах. Доступен диапазон значений от 0 до 1440.
type	Укажите тип старения.
absolute	Укажите, чтобы задать тип absolute. Все безопасные адреса на данном порту устаревают строго после указанного времени и удаляются из списка безопасных адресов. Это тип по умолчанию.
inactivity	Укажите, чтобы задать тип inactivity. Все безопасные адреса на данном порту устаревают, только если нет трафика с безопасного адреса источника в течение указанного времени.

По умолчанию

По умолчанию функция отключена.
Время хранения по умолчанию – 0 минут.

Тип хранения по умолчанию – **absolute**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для отключения процесса старения записей, а также для того, чтобы задать время старения динамически изученных безопасных записей. Для того чтобы задать тип **inactivity**, должна быть включена функция FDB Table Ageing.

Пример

В данном примере показано, как настроить время старения динамически изученных безопасных MAC-адресов для Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security aging 1
Switch(config-if)#
```

В данном примере показано, как настроить тип времени старения для Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)#
```

64-6 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 {global | vlan VLAN-ID [, | -]} VALUE
no port-security limit {global | vlan VLAN-ID [, | -]}

Параметры

global	Укажите, если необходимо применить настройки ко всей системе.
vlan VLAN-ID	Укажите необходимые VLAN ID.
,	(Опционально) Выделение серии VLAN или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон VLAN. Пробелы до и после дефиса недопустимы.
VALUE	Укажите максимальное число записей Port Security, которое может быть изучено в системе или в указанной VLAN.

Доступен диапазон значений от 1 до 12288. Если указанное значение меньше текущего числа изученных записей, команда будет отклонена.

По умолчанию

По умолчанию в данной опции ограничений нет.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет ограничить количество изученных безопасных MAC-адресов в системе или в VLAN.

Пример

В данном примере показано, как настроить максимальное число безопасных MAC-адресов для системы.

```
Switch# configure terminal
Switch(config)# port-security limit global 100
Switch(config)#
```

65. Команды энергосбережения

65-1 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 данная функция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы отключить индикаторы портов с целью энергосбережения. Используйте форму **no**, чтобы не отключать индикаторы портов с целью энергосбережения. Если данная функция включена, все индикаторы, отображающие статус порта, будут отключены с целью энергосбережения.

Пример

В данном примере показано, как отключить индикаторы портов с целью энергосбережения.

```
Switch# configure terminal
Switch(config)# dim led
Switch(config)#
```

65-2 power-saving

Данная команда используется для включения отдельных функций энергосбережения. Используйте форму **no**, чтобы отключить данные функции.

```
power-saving {link-detection | length-detection | port-shutdown | dim-led | hibernation}
no power-saving {link-detection | length-detection | port-shutdown | dim-led | hibernation}
```

Параметры

link-detection

Укажите, чтобы включать функцию энергосбережения в

	зависимости от статуса соединения.
length-detection	Укажите, чтобы включать функцию энергосбережения в зависимости от длины кабеля.
port-shutdown	Укажите, чтобы включать функцию энергосбережения по расписанию отключения индикаторов.
dim-led	Укажите, чтобы включать функцию энергосбережения по расписанию отключения порта.
hibernation	Укажите, чтобы включать функцию энергосбережения по расписанию режима сна системы. Данная функция не поддерживается коммутаторами, объединенными в физический стек.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте нижеперечисленные параметры в команде для включения/отключения отдельных функций энергосбережения:

- **link-detection** (обнаружение подключения). Энергосбережение устройства будет зависеть от неактивных портов.
- **length-detection** (обнаружение длины кабеля). Энергосбережение устройства будет зависеть от длины кабеля.
- **dim-led** (отключение индикаторов). Энергосбережение устройства будет зависеть от отключения всех индикаторов порта в указанный диапазон времени.
- **port-shutdown** (отключение порта). Энергосбережение устройства будет зависеть от отключения всех портов в указанный диапазон времени.
- **hibernation** (режим сна). Энергосбережение устройства будет зависеть от включения режима сна в указанный диапазон времени.

При включенной функции Energy-Efficient Ethernet (EEE) энергосбережение устройства будет обеспечено на портах с поддержкой EEE.

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)#
```

65-3 power-saving eee

Данная команда используется для включения функции Energy-Efficient Ethernet (EEE) на определенном порту/портах. Используйте форму **no**, чтобы отключить функцию EEE.

power-saving eee
no power-saving eee

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для включения или отключения функции Energy-Efficient Ethernet (EEE) на определенном порту/портах. В режиме Power-Saving EEE энергосбережение зависит от использования фактической пропускной способности и будет обеспечено при установленном соединении во время низкого использования трафика пакетов. Если передаваемые данные отсутствуют, на физическом интерфейсе будет включен режим Low Power Idle (LPI).

Пример

В данном примере показано, как включить функцию Power-Saving EEE.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# power-saving eee
Switch(config-if)#
```

65-4 power-saving dim-led time-range

Данная команда используется для настройки профиля временного диапазона для расписания отключения индикаторов (Dim LED). Используйте форму **no**, чтобы удалить профиль указанного диапазона времени.

power-saving dim-led time-range PROFILE-NAME
no power-saving dim-led time-range PROFILE-NAME

Параметры

PROFILE-NAME

Укажите имя профиля временного диапазона, который необходимо настроить. Максимально допустимое количество символов – 32.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы добавить/удалить профиль временного диапазона для расписания отключения индикаторов (Dim LED). Если расписание настроено, все индикаторы порта будут отключены.

Пример

В данном примере показано, как добавить профиль временного диапазона для расписания отключения индикаторов.

```
Switch# configure terminal
Switch(config)# power-saving dim-led time-range off-duty
Switch(config)#
```

65-5 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы добавить/удалить профиль временного диапазона для расписания режима сна системы (Hibernation). Когда система входит в режим сна, коммутатор начинает работать в состоянии низкого энергопотребления (режим ожидания). Отключаются все порты и не действуют сетевые функции. Будет работать только консольное соединение через порт RS232. Коммутатор, являющийся питающим устройством Power Sourcing Equipment (PSE), не будет обеспечивать порты электропитанием.

Пример

В данном примере показано, как добавить профиль временного диапазона для расписания режима сна системы.

```
Switch# configure terminal
Switch(config)# power-saving hibernation time-range off-duty
Switch(config)#
```

65-6 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы добавить/удалить профиль временного диапазона для расписания отключения порта (Port Shutdown). Если расписание настроено, указанный порт будет отключен.

Пример

В данном примере показано, как добавить профиль временного диапазона для расписания отключения порта.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# power-saving shutdown time-range off-duty
Switch(config-if)#
```

65-7 show power-saving

Данная команда используется для отображения информации о настройках энергосбережения.

```
show power-saving [link-detection] [length-detection] [dim-led] [port-shutdown] [hibernation]
[eee]
```

Параметры

link-detection	(Опционально) Укажите, чтобы отобразить настройки энергосбережения в зависимости от статуса соединения.
length-detection	(Опционально) Укажите, чтобы отобразить настройки энергосбережения в зависимости от длины кабеля.
dim-led	(Опционально) Укажите, чтобы отобразить настройки энергосбережения за счет отключения индикаторов.
port-shutdown	(Опционально) Укажите, чтобы отобразить настройки энергосбережения за счет отключения порта.
hibernation	(Опционально) Укажите, чтобы отобразить настройки энергосбережения для режима сна.
eee	(Опционально) Укажите, чтобы отобразить настройки энергосбережения для функции EEE.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Если ни один из опциональных параметров не указан, будет отображена информация о всех настройках энергосбережения.

Пример

В данном примере показано, как отобразить информацию о всех настройках энергосбережения.

```
Switch#show power-saving

Function Version: 3.00

Link Detection Power Saving
  State: Disabled

Length Detection Power Saving
  State: Disabled

Scheduled Hibernation Power Saving
  State: Disabled

Administrative Dim-LED
  State: Enabled

Scheduled Dim-LED Power Saving
  State: Disabled

Scheduled Port-shutdown Power Saving
  State: Disabled

EEE_Enabled Ports

Switch#
```

66. Команды PPPoE Circuit-ID Tag Insertion

66-1 pppoe circuit-id-insert

Данная команда используется для включения PPPoE Circuit ID Insertion.

```
pppoe circuit-id-insert  
no pppoe circuit-id- insert
```

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для глобального включения PPPoE Circuit ID Insertion. Чтобы включить PPPoE Circuit Insertion на интерфейсе, используйте команду **pppoe circuit-id-insert** в режиме Interface Configuration Mode. PPPoE Circuit ID Insertion будет включена на интерфейсе, если функция настроена и глобально, и на интерфейсе.

Если PPPoE Circuit ID Insertion включена на интерфейсе, при получении PPPoE-пакетов PADI/PADR без поля Circuit ID коммутатор вставит поле Circuit ID и перенаправит пакеты. PPPoE-пакеты PADO/PADS с полем Circuit ID будут перенаправлены только после удаления поля.

Пример

В данном примере показано, как включить PPPoE Circuit ID Insertion глобально.

```
switch# configure terminal  
switch(config)# pppoe circuit-id-insert
```

В данном примере показано, как отключить PPPoE Circuit ID Insertion глобально.

```
switch# configure terminal  
switch(config)# no pppoe circuit-id-insert
```

66-2 pppoe circuit-id-insert (interface)

Данная команда используется для включения PPPoE Circuit ID Insertion в режиме Interface Configuration Mode.

pppoe circuit-id- insert no pppoe circuit-id- insert

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить PPPoE Circuit ID Insertion на интерфейсе физического порта. PPPoE Circuit ID Insertion будет включена на интерфейсе, если функция настроена и глобально, и на интерфейсе. Для глобального включения функции используйте команду **pppoe circuit-id-insert** в режиме Global Configuration Mode.

Если PPPoE Circuit ID Insertion включена на интерфейсе, при получении PPPoE-пакетов PADI/PADR без поля Circuit ID коммутатор вставит поле Circuit ID и перенаправит пакеты. PPPoE-пакеты PADO/PADS с полем Circuit ID будут перенаправлены только после удаления поля.

Пример

В данном примере показано, как включить PPPoE Circuit ID Insertion на интерфейсе Eth1/0/1.

```
switch# configure terminal
switch(config)# interface eth1/0/1
switch(config-if)# pppoe circuit-id-insert
```

В данном примере показано, как отключить PPPoE Circuit ID Insertion на интерфейсе Eth1/0/1.

```
switch# configure terminal
switch(config)# interface eth1/0/1
switch(config-if)# no pppoe circuit-id-insert
```

66-3 pppoe circuit-id-insert format

Данная команда используется для настройки Circuit ID на определенном порту.

```
pppoe circuit-id-insert format { ip | mac | udf STRING }
no pppoe circuit-id-insert format
```

Параметры

ip	Укажите для использования IP-адреса в качестве содержимого опции Circuit ID.
-----------	--

mac	Укажите для использования MAC-адреса интерфейса VLAN управления в качестве содержимого опции Circuit ID.
udf STRING	Укажите для использования пользовательской строки в качестве содержимого опции Circuit ID. Максимально допустимое количество символов – 32.

По умолчанию

По умолчанию настроен IP-адрес коммутатора, параметр **ip**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для настройки интерфейса физического порта.

Пример

В данном примере показано, как настроить формат поля PPPoE Circuit ID на интерфейсе Eth1/1. Настроенный формат – MAC-адрес устройства.

```
switch# configure terminal
switch(config)#interface eth1/1
switch(config-if)# pppoe circuit-id-insert format mac
```

66-4 show pppoe circuit-id-insert

Данная команда используется для отображения настроек PPPoE Circuit ID Insertion.

```
show pppoe circuit-idinsert [ interface INTERFACE-ID [, | - ]]
```

Параметры

interface INTERFACE-ID	(Опционально) Укажите интерфейс или диапазон интерфейсов, настройки PPPoE Circuit ID Insertion которых 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

EXE Mode

Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения настроек PPPoE Circuit ID Insertion. Если в качестве ключевых слов в команде указан ID интерфейса(ов), будут отображены настройки указанного интерфейса/диапазона интерфейсов. Если интерфейсы не указаны, будут отображены глобальные настройки PPPoE Circuit ID Insertion.

Пример

В данном примере показано, как отобразить глобальные настройки PPPoE Circuit ID Insertion.

```
switch# show pppoe circuit-id-insert
Global PPPoE State : Enabled
```

В данном примере показано, как отобразить глобальные настройки PPPoE Circuit ID Insertion на интерфейсах Eth1/1-Eth1/4.

```
switch# show pppoe circuit-id-insert interface eth1/1-4
Interface      State      Circuit ID Type  User Defined String
-----
eth1/1         Enabled   Switch MAC
eth1/2         Enabled   Switch IP
eth1/3         Enabled   udf              12345678901234567890123456789012
eth1/4         Disabled  Switch IP
```

67. Команды Private VLAN

67-1 private-vlan

Данная команда позволяет настроить VLAN в качестве Private VLAN. При использовании формы **no** команда удалит настройку Private VLAN.

```
private-vlan {community | isolated | primary}
no private-vlan {community | isolated | primary}
```

Параметры

community	Укажите для настройки VLAN в качестве общедоступной (Community) в домене Private VLAN. Порты в Community VLAN могут обмениваться информацией друг с другом, но не с портами других Community VLAN на 2 уровне.
isolated	Укажите для настройки VLAN в качестве изолированной (Isolated) в домене Private VLAN. Порты в Isolated VLAN не могут обмениваться информацией друг с другом и с портами других Community VLAN на 2 уровне.
primary	Укажите для настройки VLAN в качестве Primary в домене Private VLAN.

По умолчанию

Нет

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Частный домен VLAN определяется одной основной (Primary) VLAN, одной изолированной (Isolated) VLAN и несколькими общедоступными (Community) VLAN. Используйте данную команду, чтобы указать роль Private VLAN перед дальнейшей настройкой Private VLAN с помощью других команд.

Пример

В данном примере показано, как настроить VLAN в качестве Private VLAN. VLAN 1000, VLAN 1001 и VLAN 1002 настроены в качестве Primary VLAN, Isolated VLAN и Community VLAN соответственно.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 1001
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 1002
Switch(config-vlan)# private-vlan community
Switch(config-vlan)#
```

67-2 private-vlan association

Данная команда позволяет ассоциировать второстепенную VLAN с основной VLAN. При использовании формы **no** команда отменит ассоциирование VLAN.

private-vlan association {add SECONDARY-VLAN-ID [, |-] | remove SECONDARY-VLAN-ID [, |-]}
no private-vlan association

Параметры

add <i>SECONDARY-VLAN-ID</i>	Укажите для связи указанной второстепенной VLAN с основной VLAN. Диапазон допустимых значений ID второстепенной VLAN: от 2 до 4094.
remove <i>SECONDARY-VLAN-ID</i>	Укажите, чтобы удалить связь указанной второстепенной сети VLAN с основной сетью VLAN.
,	(Опционально) Выделение серии VLAN или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Только одна Isolated VLAN может быть связана с основной сетью VLAN. Несколько общедоступных (Community) VLAN могут быть связаны с основной (Primary) VLAN. Второстепенная VLAN может быть связана только с одной основной (Primary) VLAN.

Пример

В данном примере показано, как связать второстепенную VLAN 1001 и второстепенную VLAN 1002 с основной VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# private-vlan association add 1001-1002
Switch(config-vlan)#
```

67-3 private-vlan synchronize

Данная команда используется для синхронизации второстепенных VLAN, чтобы иметь тот же самый идентификатор сопоставления MST (mapping MST ID), что и основная VLAN.

private-vlan synchronize

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

MST Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Второстепенные VLAN должны быть сопоставлены с теми же MST ID, что и основная VLAN, если настроена Private VLAN. Если сопоставление не синхронизировано при выходе пользователя из режима MST Configuration Mode, появится предупреждающее сообщение. Используйте команду **private-vlan synchronize**, чтобы синхронизировать сопоставление MST ID перед выходом из режима MST Configuration Mode. Данная команда не будет сохранена в текущий файл конфигурации (running configuration).

Пример

В данном примере показано, как синхронизировать сопоставление MST (MST Mapping) перед выходом из режима MST Configuration Mode.

```
Switch# configure terminal
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlans 1-100
Switch(config-mst)# instance 2 vlans 101-200
Switch(config-mst)# private-vlan synchronize
Switch(config-mst)#
```

67-4 switchport mode private-vlan

Данная команда позволяет назначить порт в качестве порта Private VLAN. Доступные типы порта – Host port (порт узла) и Promiscuous port.

switchport mode private-vlan {host | promiscuous}

Параметры

host	Укажите порт в качестве Isolated port или Community port.
promiscuous	Укажите порт в качестве Promiscuous port.

По умолчанию

По умолчанию данная опция настроена в режиме Hybrid VLAN Mode.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Для портов Isolated или Community используйте команду **switchport mode private-vlan host**, чтобы указать режим порта, и команду **switchport private-vlan host-association**, чтобы связать порт с второстепенной VLAN и основной VLAN.

Для порта Promiscuous используйте команду **switchport mode private-vlan promiscuous**, чтобы указать режим порта, и команду **switchport private-vlan mapping**, чтобы связать порт с основной VLAN и определить сопоставление с второстепенной VLAN.

При смене режима интерфейса настройки, связанные с предыдущим режимом, будут утеряны.

Пример

В данном примере показано, как настроить физические порты в качестве портов Private VLAN. Здесь Ethernet 1/0/1 указан как Host Port для Private VLAN, а Ethernet 1/0/2 указан как Promiscuous Port для Private VLAN.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# exit
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)#
```

67-5 switchport private-vlan host-association

Данная команда используется для связи Private VLAN с портом Isolated, портом Community или второстепенным портом Trunk. При использовании формы **no** команда отменит связь.

switchport private-vlan host-association PRIMARY-VLAN-ID SECONDARY-VLAN-ID

no switchport private-vlan host-association**Параметры**

<i>PRIMARY-VLAN-ID</i>	Укажите ID основной VLAN, которую необходимо ассоциировать. Диапазон доступных ID: от 2 до 4094.
<i>SECONDARY-VLAN-ID</i>	Укажите ID второстепенной VLAN, которую необходимо ассоциировать. Диапазон доступных ID: от 2 до 4094.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Порт является Isolated портом, если второстепенная VLAN, указанная в команде, будет являться Isolated VLAN. Порт является Community портом, если второстепенная VLAN, указанная командой, является Community VLAN.

Пример

В данном примере показано, как связать Ethernet 1/0/1 с основной VLAN 1000 и второстепенной VLAN 1001.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 1000 1001
Switch(config-if)#
```

67-6 switchport private-vlan mapping

Данная команда позволяет ассоциировать членство Private VLAN с портом Promiscuous или Trunk Promiscuous. При использовании формы **no** команда отменит ассоциирование.

```
switchport private-vlan mapping PRIMARY-VLAN-ID {add SECONDARY-VLAN-ID [, | -]} | remove
SECONDARY-VLAN-ID [, | -]}
no switchport private-vlan mapping
```

Параметры

add <i>SECONDARY-VLAN-ID</i>	Укажите, чтобы добавить членство в указанной второстепенной VLAN. Диапазон доступных ID Secondary VLAN: от 2 до 4094.
remove <i>SECONDARY-VLAN-ID</i>	Укажите, чтобы удалить членство в указанной второстепенной VLAN.

,	(Опционально) Выделение серии VLAN или разделение группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально) Укажите диапазон VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда доступна для физического порта и настройки интерфейса port-channel.

Команда настроит порт в качестве нетегированного члена указанной основной VLAN и маркировки второстепенной VLAN.

Пример

В данном примере показано, как настроить Ethernet 1/0/2 в качестве порта Promiscuous для Private VLAN и сопоставить его с основной VLAN 1000 и второстепенными VLAN 1001 и VLAN 1002.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 1000 add 1001,1002
Switch(config-if)#
```

67-7 show vlan private-vlan

Данная команда используется для просмотра настроек Private VLAN.

show vlan private-vlan

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Команда используется для отображения списка Private VLAN, находящегося в домене VLAN, ассоциации второстепенного VLAN с основным VLAN и портов каждого Private VLAN.

Пример

В данном примере показано, как включить отображение настроек Private VLAN. В данном примере настроено 2 домена Private VLAN.

```
Switch#show vlan private-vlan

Primary VLAN   Secondary VLAN   Type             Interface
-----
1000           1001             Isolated         eth1/0/1, eth1/0/16
                1002             Community
                1003             Community
2000           2001             Isolated         eth1/0/2, eth1/0/3
2000           2002             Community        eth1/0/2, eth1/0/5
2000           2003             Community        eth1/0/4, eth1/0/13, eth1/0/15

Total Entries: 6

Switch#
```

68. Команды Protocol Independent

68-1 distance

Данная команда используется для настройки административного расстояния (Administrative Distance) для протоколов маршрутизации, включая RIP and BGP. Используйте форму по, чтобы вернуться к настройкам по умолчанию.

distance *DISTANCE*
no distance

Параметры

<i>DISTANCE</i>	Укажите административное расстояние. Доступный диапазон значений: от 1 до 255.
-----------------	--

По умолчанию

Расстояние подключенного маршрута по умолчанию – 0.
 Расстояние маршрута протокола External Border Gateway Protocol (eBGP) по умолчанию – 70.
 Расстояние Intra-area Route протокола Open Shortest Path First (OSPF) по умолчанию – 80.
 Расстояние Inter-area Route протокола OSPF по умолчанию – 90.
 Расстояние **Type-1 AS External Route** протокола OSPF по умолчанию – 110.
 Расстояние **Type-2 AS External Route** протокола OSPF по умолчанию – 115.
 Расстояние Internal **Route** протокола BGP по умолчанию – 130.

Режим ввода команды

Router Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить расстояние, которое представляет рейтинг доверия маршрута. В качестве расстояния может быть указано целое число от 1 до 255. Маршрут, значение расстояния которого ниже, имеет более высокий приоритет, чем маршрут со значением выше. Маршруты, расстояние которых равно 255, не будут установлены для маршрутизации пакетов, поскольку в данном случае маршруты не являются доверенными. Если команда используется без параметров, указанным расстоянием будет значение маршрута по умолчанию настроенного протокола.

Пример

В данном примере показано, как настроить расстояние маршрута RIP. Настроенное расстояние – 75.

```
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#distance 75
Switch(config-router)#
```

68-2 distance default

Данная команда используется для настройки административного расстояния для статического маршрута по умолчанию. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

distance default *DISTANCE*
no distance default

Параметры

<i>DISTANCE</i>	Укажите административное расстояние. Доступный диапазон значений: от 1 до 255.
-----------------	--

По умолчанию

Расстояние статического маршрута по умолчанию – 1.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить расстояние, которое представляет рейтинг доверия маршрута. В качестве расстояния может быть указано целое число от 1 до 255. Маршрут, значение расстояния которого ниже, имеет более высокий приоритет, чем маршрут со значением выше. Маршруты, расстояние которых равно 255, не будут установлены для маршрутизации пакетов, поскольку в данном случае маршруты не являются доверенными. Если команда используется без параметров, указанным расстоянием будет значение маршрута по умолчанию настроенного протокола.

Пример

В данном примере показано, как настроить расстояние статического маршрута по умолчанию. Настроенное расстояние – 150.

```
Switch#configure terminal
Switch(config)#distance default 150
Switch(config)#
```

68-3 distance static

Данная команда используется для настройки административного расстояния для статических маршрутов. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

distance static *DISTANCE*
no distance static

Параметры

<i>DISTANCE</i>	Укажите административное расстояние. Доступный диапазон значений: от 1 до 255.
-----------------	--

По умолчанию

Расстояние статического маршрута по умолчанию – 60.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить расстояние, которое представляет рейтинг доверия маршрута. В качестве расстояния может быть указано целое число от 1 до 255. Маршрут, значение расстояния которого ниже, имеет более высокий приоритет, чем маршрут со значением выше. Маршруты, расстояние которых равно 255, не будут установлены для маршрутизации пакетов, поскольку в данном случае маршруты не являются доверенными. Если команда используется без параметров, указанным расстоянием будет значение маршрута по умолчанию настроенного протокола.

Пример

В данном примере показано, как настроить расстояние статического маршрута. Настроенное расстояние – 100.

```
Switch# configure terminal
Switch(config)# distance static 100
Switch(config)#
```

68-4 distribute-list in

Данная команда используется для настройки Distribute List для фильтрации обновлений маршрута протокола на основе указанного списка доступа. Используйте форму **no**, чтобы удалить фильтр.

```
distribute-list ACCESS-LIST-NAME in [INTERFACE-ID]
no distribute-list ACCESS-LIST-NAME in [INTERFACE-ID]
```

Параметры

<i>ACCESS-LIST-NAME</i>	Укажите имя стандартного списка доступа IP, определяющего, какие полученные обновления маршрута должны быть приняты, а какие – анонсированы.
<i>INTERFACE-ID</i>	(Опционально) Укажите интерфейс, к которому необходимо применить настроенный Distribute List.

По умолчанию

Нет

Режим ввода команды

Router Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если список доступа был применен к интерфейсу с использованием **distribute-list in** в команде, обновления маршрута, полученные указанным интерфейсом, фильтруются на основе списка доступа.

Если ID интерфейса указан, Distribute List будет применен к указанному интерфейсу. Если ID интерфейса не указан, Distribute List будет применен ко всем интерфейсам.

Пример

В данном примере показано, как настроить список доступа для фильтрации обновлений маршрута протокола RIP. Настроенный список доступа – East-ranch.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# distribute-list East-ranch in
Switch(config-router)#
```

68-5 ip route

Данная команда используется для создания записи статического маршрута. Используйте форму **no**, чтобы удалить запись статического маршрута.

ip route *NETWORK-PREFIX NETWORK-MASK* {*IP-ADDRESS* [**primary** | **backup** | **weight** *NUMBER*] | **null0**}
IP-TUNNEL-NAME
no ip route *NETWORK-PREFIX NETWORK-MASK* {*IP-ADDRESS* | **null0**} *IP-TUNNEL-NAME*

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.
primary	(Опционально) Укажите маршрут как основной маршрут к назначению.
backup	(Опционально) Укажите маршрут как резервный маршрут к назначению.
null0	Укажите маршрут Black Hole Route.
<i>IP-TUNNEL-NAME</i>	Укажите туннель в качестве следующего узла.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте **0.0.0.0 0.0.0.0**, чтобы указать маршрут по умолчанию.

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)#
```

68-6 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]] [DISTANCE]}
no ipv6 route {default | NETWORK-PREFIX/PREFIX-LENGTH} {[INTERFACE-ID] NEXT-HOP-ADDRESS}
```

Параметры

default	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.
primary	(Опционально) Укажите маршрут как основной маршрут к назначению.
backup	(Опционально) Укажите маршрут как резервный маршрут к назначению.
<i>DISTANCE</i>	(Опционально) Укажите административное расстояние

статического маршрута. Доступный диапазон значений: от 1 до 254. Чем ниже значение, тем выше приоритет маршрута. Если значение не указано, административный путь статического маршрута по умолчанию – 1.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Доступны плавающие маршруты. Это означает, что можно создать два маршрута с одним адресом сети назначения, но с разными следующими узлами (Next Hop). Если ни один из параметров (**primary** или **backup**) не указан, роль статического маршрута (основной/резервный) будет назначена автоматически. 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 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)#
```

68-7 ip route ecmp advance-control mode

Данная команда используется для увеличения или уменьшения значения ECMP (многопутевой маршрутизации). Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip route ecmp advance-control mode {VALUE1 | VALUE2 | VALUE3 | VALUE4 | VALUE5}
no ip route ecmp advance-control mode
```

Параметры

<i>VALUE1 ... VALUE5</i>	Укажите значение ECMP (многопутевой маршрутизации) и количество следующих узлов (Next Hop) каждого ECMP, чтобы изменить их в соответствии с указанным значением. Доступные значения: 1024, 512, 256, 128 и 64.
--------------------------	---

По умолчанию

Значение по умолчанию – 128.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для увеличения или уменьшения значения ECMP (многопутевой маршрутизации).

Пример

В данном примере показано, как настроить значение ECMP (многопутевой маршрутизации). Настроенное значение – 512.

```
Switch#configure terminal
Switch(config)#ip route ecmp advance-control mode 512

WARNING: The command does not take effect until after the next reboot.
Switch(config)#
```

68-8 ip route ecmp load-balance

Данная команда используется для настройки хэш-алгоритма балансировки нагрузки для определения записи следующего узла (Next Hop) из разных путей для достижения одного назначения. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip route ecmp load-balance {{sip | crc32_lower | crc32_upper} | dip | port}
no ip route ecmp load-balance {{sip | crc32_lower | crc32_upper} | dip | port}
```

Параметры

sip	Укажите алгоритм балансировки нагрузки, включающий младшие 5 бит IP-адреса источника. Данный параметр и crc32_lower/crc32_upper являются взаимоисключающими. При указании sip параметры crc32_lower и crc32_upper будут отменены.
crc32_lower	Укажите алгоритм балансировки нагрузки, включающий младшие 5 бит CRC. Данный параметр и crc32_upper/sip являются взаимоисключающими. При указании crc32_lower параметры crc32_upper и sip будут отменены.
crc32_upper	Укажите алгоритм балансировки нагрузки, включающий старшие 5 бит CRC. Данный параметр и crc32_lower/sip являются взаимоисключающими. При указании crc32_upper параметры crc32_lower и sip будут отменены.
dip	Укажите алгоритм балансировки нагрузки, включающий IP-адрес назначения.
port	Укажите алгоритм балансировки нагрузки, включающий TCP-порт или UDP-порт.

По умолчанию

По умолчанию используется параметр `rip`.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки хэш-алгоритма балансировки нагрузки для определения записи следующего узла (Next Hop) из разных путей для достижения одного назначения.

Пример

В данном примере показано, как настроить алгоритм балансировки нагрузки. Настроенный алгоритм – `dir`.

```
Switch#configure terminal
Switch(config)#ip route ecmp load-balance dir
Switch(config)#
```

68-9 show ip protocols

Данная команда используется для отображения состояния процесса маршрутизации.

show ip protocols [rip]

Параметры

rip	(Опционально) Укажите, чтобы полностью отобразить настройки протокола RIP.
------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить состояние процессов маршрутизации. Если ни один из параметров не указан, отображаются все текущие процессы маршрутизации.

Пример

В данном примере показано, как отобразить информацию о протоколе маршрутизации.

```
Switch#show ip protocols

Routing Protocol is RIP
  Sending updates every 10 seconds, next due in 5 seconds
  Invalid 80 secs, flush 160 secs
  Default redistribution metric is 0
  Default version control: send version 1, receive any version
  Interface      Send      Recv
  vlan 11        1         1 2
  vlan 1         1         1 2
Maximum path: 1
Routing for Networks:
  vlan 11 (11.0.0.3/255.0.0.0)
  vlan 1  (107.100.0.1/255.255.0.0)
Routing Information Sources:
  Gateway        Last Update
  11.0.0.2       22:54:09
  11.0.0.5       22:53:59
  11.0.0.254    22:53:51
Distribute list:
  East branch (in)
  Interface      in
Distance:100

Switch#
```

68-10 show ip route

Данная команда используется для отображения записи в таблице маршрутизации.

```
show ip route [[IP-ADDRESS [MASK] | PROTOCOL]]
```

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.
<i>PROTOCOL</i>	(Опционально) Укажите протокол маршрутизации или ключевые слова: static , connected .

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

В таблицу маршрутизации занесены маршруты, информация о которых была получена из разных протоколов. При достижении одной сети несколькими маршрутами для маршрутизации пакетов будет назначен лучший маршрут, расстояние которого имеет более высокий приоритет, а следующий узел доступен. Расстояние и следующий узел (Next Hop) являются текущей записью маршрута. То есть, если следующий узел маршрута с самым приоритетным расстоянием недоступен, данный маршрут будет заменен другим маршрутом, расстояние которого будет следующим по значению приоритета.

Пример

В данном примере показано, как отобразить таблицу маршрутизации.

```
Switch#show ip route
Code: C - connected, S - static, R - RIP, B - BGP, I - IS-IS, O - OSPF,
      IA - OSPF inter area,
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2,
      E1 - OSPF external type 1, E2 - OSPF external type 2,
      * - candidate default

Gateway of last resort is not set

S    170.10.0.0/16 [60/1] via 11.0.0.2, vlan 11
O    1.0.0.0/8 [80/2] via 11.0.0.1, vlan 11
O    2.0.0.0/8 [80/2] via 11.0.0.1, vlan 11
C    11.0.0.0/8 is directly connected, vlan 11
O    12.0.0.0/8 [80/3] via 11.0.0.1, vlan 11
O    13.0.0.0/8 [80/3] via 11.0.0.1, vlan 11
O    17.0.0.0/8 [80/3] via 11.0.0.1, vlan 11
O    18.0.0.0/8 [80/3] via 11.0.0.1, vlan 11
O    30.0.0.0/8 [80/2] via 11.0.0.1, vlan 11
O    40.0.0.0/8 [80/3] via 11.0.0.1, vlan 11
I    41.0.0.0/8 [116/10] via 11.0.0.2, vlan 11
R    105.100.0.0/24 [100/2] via 11.0.0.5, vlan 11
C    107.100.0.0/16 is directly connected, vlan 1
C    172.18.64.0/21 is directly connected, mgmt_ipif
R    212.254.254.0/24 [100/2] via 11.0.0.254, vlan 11

Total Entries: 15

Switch#
```

68-11 show ip route summary

Данная команда используется для отображения краткой информации о текущих записях маршрутизации.

show ip route summary

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения краткой информации о текущих записях маршрутизации.

Пример

В данном примере показано, как отобразить краткую информацию о текущих записях маршрутизации.

```
Switch#show ip route summary
Route Source    Networks
Connected       3
Static          1
RIP             2
OSPF            8
BGP             0
ISIS           1
Total          15
Multi-path      0
Switch#
```

68-12 show ipv6 route

Данная команда используется для отображения записи в таблице маршрутизации.

show ipv6 route *[[IPV6-ADDRESS | NETWORK-PREFIX/PREFIX-LENGTH | INTERFACE-ID | PROTOCOL] [database]]*

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.

<i>INTERFACE-ID</i>	(Опционально) Укажите тип интерфейса.
<i>PROTOCOL</i>	(Опционально) Укажите протокол маршрутизации.
database	(Опционально) Укажите, чтобы отобразить все связанные записи в базе данных маршрутизации, а не только самый приоритетный маршрут.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

В таблицу маршрутизации занесены маршруты, информация о которых была получена из разных протоколов. При достижении одной сети несколькими маршрутами для маршрутизации пакетов будет назначен лучший маршрут, расстояние которого имеет более высокий приоритет, а следующий узел доступен. Расстояние и следующий узел (Next Hop) являются текущей записью маршрута. То есть, если следующий узел маршрута с самым приоритетным расстоянием недоступен, данный маршрут будет заменен другим маршрутом, расстояние которого будет следующим по значению приоритета.

Пример

В данном примере показано, как отобразить записи маршрутизации для IPv6.

```
Switch#show ipv6 route summary

Route Source   Networks
Connected      2
Static         1
RIPng          7
BGP            0
OSPF           4
ISIS           2
SLAAC          0
Total          16
Switch#
```

68-13 show ipv6 route summary

Данная команда используется для отображения текущего состояния таблицы маршрутизации IPv6.

```
show ipv6 route summary
```

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Если система обслуживания обеспечивает продвижение IPv6-трафика, необходимо проверять таблицу преадресации/маршрутизации для выявления пути трафика, который будет использоваться в сети.

Пример

В данном примере показано, как отобразить текущее состояние таблицы маршрутизации IPv6.

```
Switch#show ipv6 route summary
```

```
Route Source    Networks
Connected       2
Static          1
RIPng           7
BGP             0
OSPF            4
ISIS            2
SLAAC           0
Total           16
Switch#
```

69. Команды качества обслуживания (QOS)

69-1 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

Уровень команды по умолчанию

Уровень 12

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)#
```


69-2 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.
match-any	(Опционально) Укажите, чтобы критерии соответствия карты класса были оценены на основе логического OR. Если ключевое слово match-all или match-any не указано, по умолчанию будет использовано match-any .
match-all	(Опционально) Укажите, чтобы критерии соответствия карты класса были оценены на основе логического AND. Если ключевое слово match-all или match-any не указано, по умолчанию будет использовано match-any .

По умолчанию

По умолчанию используется только Class-Default.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы создать или изменить карту класса, в которой определены критерии соответствия пакетов, настраиваемые в режиме Class-map Configuration Mode.

Если для класса настроено несколько команд соответствия, необходимо использовать ключевое слово **match-all** или **match-any**, чтобы указать, на основе чего (логического AND или логического OR) будут оцениваться критерии соответствия.

Пример

В данном примере показано, как настроить имя карты класса. Настроенное имя – class_home_user. Условие соответствия для данной карты класса выполняется, если трафик, соответствующий списку управления доступом «acl_home_user» и протоколу IPv6, будет включен в настроенную карту класса «class_home_user».

```
Switch# configure terminal
Switch(config)# class-map match-all class_home_user
Switch(config-map)# match access-group name acl_home_user
Switch(config-map)# match protocol ipv6
Switch(config-map)#
```

69-3 match

Данная команда используется для настройки критериев соответствия для карты класса. Используйте форму **no**, чтобы удалить критерии соответствия.

match {**access-group name** *ACCESS-LIST-NAME* | **cos** [**inner**] *COS-LIST* | [**ip**] **dscp** *DSCP-LIST* | [**ip**] **precedence** *IP-PRECEDENCE-LIST* | **protocol** *PROTOCOL-NAME* | **vlan** [**inner**] *VLAN-LIST*}

no match {**access-group name** *ACCESS-LIST-NAME* | **cos** [**inner**] *COS-LIST* | [**ip**] **dscp** *DSCP-LIST* | [**ip**] **precedence** *IP-PRECEDENCE-LIST* | **protocol** *PROTOCOL-NAME* | **vlan** [**inner**] *VLAN-ID-LIST*}

Параметры

access-group name <i>ACCESS-LIST-NAME</i>	Укажите список доступа в качестве критерия соответствия. Трафик, разрешенный указанным списком доступа, будет классифицирован.
cos [inner] <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. inner – (Опционально) Укажите, чтобы сопоставить внутренний CoS пакетов QinQ с маркировкой 2 уровня класса обслуживания (Class of Service, CoS).
[ip] dscp <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. ip – (Опционально) Укажите, чтобы настроить критерий соответствия только для пакетов IPv4. Если не указано, проверка критерий настраивается для пакетов IPv4 и IPv6.
[ip] precedence <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. ip – (Опционально) Укажите, чтобы настроить критерий соответствия только для пакетов IPv4. Если не указано, критерий соответствия настраивается для пакетов IPv4 и IPv6. Для пакетов IPv6 приоритетом являются три наиболее значимых бита класса трафика заголовка IPv6.
protocol <i>PROTOCOL-NAME</i>	Укажите имя протокола в качестве критерия соответствия.
vlan [inner] <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.

inner – (Опционально) Укажите, чтобы настроить критерий соответствия внутреннего VLAN ID в кадре с двойным тегом 802.1Q.

По умолчанию

Нет

Режим ввода команды

Class-map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Перед применением данной команды используйте команду **class-map**, чтобы указать имя класса, для которого будут настроены критерии соответствия. Политика обработки данных соответствующих пакетов настраивается в режиме Policy-map Class Configuration Mode.

В списке ниже представлены протоколы, доступные для данной команды:

- **arp** - IP Address Resolution Protocol (ARP)
- **bgp** - Border Gateway Protocol
- **dhcp** - Dynamic Host Configuration
- **dns** - Domain Name Server lookup
- **egp** - Exterior Gateway Protocol
- **ftp** - File Transfer Protocol
- **ip** - IP (version 4)
- **ipv6** - IP (version 6)
- **netbios** – NetBIOS
- **nfs** - Network File System
- **ntp** - Network Time Protocol
- **ospf** - Open Shortest Path First
- **pppoe** - Point-to-Point Protocol over Ethernet
- **rip** - Routing Information Protocol
- **rtsp** - Real-Time Streaming Protocol
- **ssh** - Secured shell
- **telnet** – Telnet
- **tftp** - Trivial File Transfer Protocol

Пример

В данном примере показано, как настроить карту класса и список доступа, который будет использован в качестве критерия соответствия для данного класса. Имя настроенной карты класса – class-home-user. Имя настроенного списка доступа – acl-home-user.

```
Switch# configure terminal
Switch(config)# class-map class-home-user
Switch(config-cmap)# match access-group name acl-home-user
Switch(config-cmap)#
```

В данном примере показано, как настроить карту класса и значения CoS, которые будут использованы в качестве критериев соответствия для данного класса. Имя настроенной карты класса – `cos`. Настроенные значения CoS – 1, 2 и 3.

```
Switch# configure terminal
Switch(config)# class-map cos
Switch(config-cmap)# match cos 1,2,3
Switch(config-cmap)#
```

В данном примере показано, как настроить классы для классификации трафика на основе значений CoS. Имена настроенных классов: `voice` и `video-n-data`. Обработка QoS предназначена для соответствующих пакетов в карте политики «`cos-based-treatment`». Для обработки QoS класса «`voice`» используется Single Rate Policer, для класса «`video-n-data`» – Two Rate Policer. Настроенная политика обслуживания привязана к интерфейсу Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# class-map voice
Switch(config-cmap)# match cos 7
Switch(config-cmap)# exit
Switch(config)# class-map video-n-data
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
Switch(config)# policy-map cos-based-treatment
Switch(config-pmap)# class voice
Switch(config-pmap-c)# police 8000 1000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video-n-data
Switch(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 exceed-action set-dscp-transmit 2 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# service-policy input cos-based-treatment
Switch(config-if)#
```

69-4 mls qos aggregate-policer

Данная команда используется для настройки Aggregate Policer, который будет использован в картах политики. Используйте форму `no`, чтобы удалить Aggregate Policer. Команда **`mls qos aggregate-policer`** применяется для использования Single Rate Policing, а команда **`mls qos aggregate-policer cir`** для использования Two Rate Policing.

```
mls qos aggregate-policer NAME KBPS [BURST-NORMAL [BURST-MAX]] [conform-action ACTION]
exceed-action ACTION [violate-action ACTION] [color-aware]
mls qos aggregate-policer NAME cir CIR [bc CONFORM-BURST] pir PIR [be PEAK-BURST][conform-
action ACTION] [exceed-action ACTION [violate-action ACTION]] [color-aware]
no mls qos aggregate-policer NAME
```

Параметры

<i>NAME</i>	Укажите имя правила Aggregate Policing. Максимально допустимое количество символов – 32. Символы,
-------------	---

	используемые в данном параметре, чувствительны к регистру. Имена Aggregate Policer не должны совпадать и начинаться с цифры. Первым символом в имени обязательно должна быть буква.
<i>KBPS</i>	Укажите среднюю скорость в Кбит/с.
<i>BURST-NORMAL</i>	(Опционально) Укажите нормальный размер всплеска (Burst). Единица измерения – Кбайт.
<i>BURST-MAX</i>	(Опционально) Укажите максимальный размер всплеска (Burst). Единица измерения – Кбайт.
<i>CIR</i>	Укажите гарантированную полосу пропускания (Committed Information Rate) в Кбит/с. Данный параметр является первым в алгоритме «корзина маркеров» (Token Bucket) для Two-rate Metering.
<i>PIR</i>	Укажите пиковую скорость передачи (Peak Information Rate) в Кбит/с. Данный параметр является вторым в алгоритме «корзина маркеров» (Token Bucket) для Two-rate Metering.
<i>PEAK-BURST</i>	(Опционально) Укажите размер всплеска (Burst) для первого параметра алгоритма «корзина маркеров» (Token Bucket). Единица измерения – Кбайт.
conform-action	(Опционально) Укажите, чтобы действие было выполнено к Green Color Packets (пакетам, «окрашенным» в зелёный цвет). Если не указано, будет выполнено действие по умолчанию transmit (передача пакетов).
exceed-action	Укажите, чтобы действие было выполнено к пакетам, превышающим разрешенную скорость. Если при использовании Two Rate Policer данный параметр не указан, будет выполнено действие по умолчанию drop (отбрасывание).
violate-action	(Опционально) Укажите, чтобы при использовании Single Rate Policing действие было выполнено к пакетам, нормальный и максимальный размеры всплеска которых не соответствуют заданным параметрам. Укажите, чтобы действие было выполнено к пакетам, не соответствующим обоим параметрам CIR и PIR. Если при использовании Single Rate Policer данный параметр не указан, будет создан Single Rate Two Color Policer. Если при использовании Two Rate Policer данный параметр не указан, будет выполнено действие по умолчанию drop (отбрасывание).
<i>ACTION</i>	Укажите, чтобы действие было выполнено к пакетам. Ниже указаны ключевые слова: drop – отбрасывание пакетов. set-dscp-transmit VALUE – укажите значение IP DSCP-метки и передачу пакетов с новой IP DSCP-меткой. set-1p-transmit – укажите значение 802.1p и передачу пакетов с новым значением. transmit – передача пакетов без изменений.
color-aware	(Опционально) Укажите данный параметр для Single Rate Three Color Policer или Two Rate Three Color Policer. Если данный параметр не указан, Policer работает в режиме Color Blind. Если данный параметр указан, Policer работает в режиме Color Aware.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Aggregate Policer может быть общим для разных классов в карте политики. Для разных карт политики настройка общего Aggregate Policer невозможна.

Пример

В данном примере показано, как настроить Aggregate Policer с использованием Single Rate Two Color Policer. Настроенное имя Aggregate Policer – agg-policer5. Данный Aggregate Policer применен в качестве политики обслуживания для классов трафика 1 и 2 (class1, class2) в карте политики «policy 2».

```
Switch# configure terminal
Switch(config)# mls qos aggregate-policer agg-policer5 10 1000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer5
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police aggregate agg_policer5
Switch(config-pmap-c)#
```

69-5 mls qos cos

Данная команда используется для настройки значения CoS по умолчанию для порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
mls qos cos {COS-VALUE | override}
no mls qos cos
```

Параметры

COS-VALUE	Укажите значение CoS по умолчанию, которое будет применено к входящим нетегированным пакетам, полученным на порту.
override	Укажите, чтобы отменить CoS пакетов. Для всех полученных на порту пакетов (тегированных и нетегированных) будет применен CoS по умолчанию.

По умолчанию

Значение CoS по умолчанию – 0.
По умолчанию параметр **override** не указан.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если параметр **override** не указан, для тегированных пакетов применяется CoS, назначенный пакету; для нетегированных пакетов будет применен CoS по умолчанию.

Если параметр **override** указан, для всех полученных на порту пакетов будет применен CoS по умолчанию. Используйте ключевое слово **override**, если все входящие пакеты на определенных портах заслуживают приоритет выше или ниже, чем пакеты, поступающие из других портов. При использовании данной команды, ранее настроенные доверенные DSCP и CoS будут перезаписаны, и все значения CoS входящих пакетов будут изменены на CoS по умолчанию, настроенный в команде **mls qos cos**. Если входящие пакеты тегированные, их значение CoS изменяется на входном порту.

CoS по умолчанию пакетов, поступающих на порт 802.1Q VLAN tunnel, имеет два значения: внутренний CoS, назначенный пакету, и CoS в теге VLAN tunnel передаваемого пакета.

Пример

В данном примере показано, как настроить значение CoS по умолчанию на Ethernet-порту 1/0/1. Настроенное значение – 3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# mls qos cos 3
Switch(config-if)#
```

69-6 mls qos dscp-mutation

Данная команда используется для привязки карты изменения входящего DSCP (DSCP Mutation) к интерфейсу. Используйте форму **no**, чтобы удалить привязку карты DSCP Mutation к интерфейсу.

```
mls qos dscp-mutation DSCP-MUTATION-TABLE-NAME
no mls qos dscp-mutation
```

Параметры

<i>DSCP-MUTATION-TABLE-NAME</i>	Укажите имя таблицы DSCP Mutation без пробелов. Максимально допустимое количество символов – 32.
---------------------------------	---

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы привязать таблицу DSCP Mutation к интерфейсу. Значение DSCP пакета, полученного на интерфейсе, будет изменено с помощью DSCP Mutation. Пакет с новым значением DSCP будет обработан QoS и отправлен из порта коммутатора.

Пример

В данном примере показано, как преобразовать значение DSCP и привязать карту изменений внутреннего DSCP (DSCP Mutation) к порту Ethernet 1/0/1. Ранее настроенное значение DSCP – 30. Новое значение – 8. Карта DSCP Mutation – mutemap1.

```
Switch# configure terminal
Switch(config)# mls qos map dscp-mutation mutemap1 30 to 8
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# mls qos dscp-mutation mutemap1
Switch(config-if)#
```

69-7 mls qos map cos-color

Данная команда используется для настройки цветовой привязки CoS пакета. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
mls qos map cos-color COS-LIST to {green | yellow | red}
no mls qos map cos-color
```

Параметры

<i>COS-LIST</i>	Укажите список значений CoS для привязки к цвету. Доступный диапазон значений: от 0 до 7. Несколько значений CoS могут быть отделены запятой или списком диапазонов.
green	Укажите для привязки к зеленому цвету.
yellow	Укажите для привязки к желтому цвету.
red	Укажите для привязки к красному цвету.

По умолчанию

По умолчанию все значения CoS привязаны к зеленому цвету.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Пакеты, поступающие на входной порт, могут быть «окрашены» на основе цветовой привязки DSCP (если порт является доверенным портом DSCP) или на основе цветовой привязки CoS (если порт является доверенным портом CoS).

Используйте данную команду в режиме Interface Configuration Mode, чтобы настроить цветовую привязку CoS. Если входной порт является доверенным портом CoS, полученный пакет будет инициализирован с цветом на основе настроенной привязки.

Пример

В данном примере показано, как настроить цветовую привязку CoS пакетов, поступающих на интерфейс Ethernet 1/0/1. Пакеты со значением CoS от 1 до 7 привязаны к красному цвету, а пакеты со значением 0 – к зеленому.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# mls qos map cos-color 1-7 to red
Switch(config-if)#
```

69-8 mls qos map dscp-color

Данная команда используется для настройки цветовой привязки DSCP пакета. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
mls qos map dscp-color DSCP-LIST to {green | yellow | red}
no mls qos map dscp-color DSCP-LIST
```

Параметры

<i>DSCP-LIST</i>	Укажите список DSCP-меток для привязки к цвету. Доступный диапазон значений: от 0 до 63. Несколько значений DSCP могут быть отделены запятой или списком диапазонов.
green	Укажите для привязки к зеленому цвету.
yellow	Укажите для привязки к желтому цвету.
red	Укажите для привязки к красному цвету.

По умолчанию

По умолчанию привязка не настроена. Все значения DSCP привязаны к зеленому цвету.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки цветовой привязки DSCP пакета.

Пример

В данном примере показано, как привязать пакеты с DSCP-меткой от 61 до 63 к желтому цвету на интерфейсе Ethernet 1/0/1. Другие IP-пакеты будут инициализированы с зеленым цветом.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# mls qos map dscp-color 61-63 to yellow
Switch(config-if)#
```

69-9 mls qos map dscp-cos

Данная команда используется для привязки DSCP-меток к CoS. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
mls qos map dscp-cos DSCP-LIST to COS-VALUE
no mls qos map dscp-cos DSCP-LIST
```

Параметры

dscp-cos <i>DSCP-LIST</i> to <i>COS-VALUE</i>	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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда позволяет привязать DSCP-метку доверенного порта DSCP к значению внутреннего CoS. Данное значение CoS будет привязано к очереди CoS на основе CoS в карте очереди, настроенной в команде **priority-queue cos-map**.

Пример

В данном примере показано, как привязать DSCP к CoS на интерфейсе Ethernet 1/0/6. DSCP-метки 12, 16 и 18 привязаны к CoS 1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/6
Switch(config-if)# mls qos map dscp-cos 12,16,18 to 1
Switch(config-if)#
```

69-10 mls qos map dscp-mutation

Данная команда используется для настройки карты DSCP Mutation. Используйте форму **no**, чтобы удалить карту Mutation.

```
mls qos map dscp-mutation MAP-NAME INPUT-DSCP-LIST to OUTPUT-DSCP
no mls qos map dscp-mutation MAP-NAME
```

Параметры

<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

По умолчанию параметры *OUTPUT-DSCP* и *INPUT-DSCP* равны.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Значение внутреннего DSCP пакета, полученного на интерфейсе, будет изменено на основе карты DSCP Mutation перед другими QoS-операциями. DSCP Mutation способствует объединению доменов с разными назначениями DSCP.

При настройке карты DSCP Mutation обратите внимание на то, что для каждого нового значения DSCP, которых нужно изменить, и для каждого нового значения, которые будут применены после «мутации» Mutation, необходимо использовать команду несколько раз.

Привязки DSCP-CoS и DSCP-color будут основываться на исходном DSCP пакета, а все последующие действия – на значении DSCP, которое будет применено после «мутации» Mutation.

Пример

В данном примере показано, как преобразовать DSCP 30 в DSCP 8 и DSCP 20 в DSCP 10. Имя карты Mutation – mutemap1.

```
Switch# configure terminal
Switch(config)# mls qos map dscp-mutation mutemap1 30 to 8
Switch(config)# mls qos map dscp-mutation mutemap1 20 to 10
Switch(config)#
```

69-11 mls qos scheduler

Данная команда используется для настройки механизма обслуживания очередей. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
mls qos scheduler {sp | rr | wrr | wdr}
no mls qos scheduler
```

Параметры

sp	Укажите алгоритм Strict Priority, SP для всех очередей.
rr	Укажите алгоритм Round-Robin, RR для всех очередей.
wrr	Укажите алгоритм Weighted Round-Robin, WRR по числу кадров для всех очередей. Если настроенный вес (Weight) очереди равен нулю, для данной очереди будет включен алгоритм Strict Priority, SP.
wdr	Укажите алгоритм Weighted Deficit Round-Robin, WDRR по длине кадров (Quantum) для очередей всех портов. Если настроенный вес (Weight) очереди равен нулю, для данной очереди включен алгоритм Strict Priority, SP.

По умолчанию

Алгоритм механизма обслуживания очередей для очереди по умолчанию – WRR.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Укажите алгоритм обслуживания очередей (WRR, SP, RR или WDRR) для выходной очереди. Алгоритм обслуживания очередей для очереди по умолчанию – WRR. WDRR предназначен для набора накопившихся кредитов в очереди передачи в режиме Round-Robin. Изначально для каждой очереди установлен свой счетчик кредита (настроенное значение Quantum). Каждый раз, когда пакет отправляется из очереди CoS, размер пакета вычитается из соответствующего счетчика кредитов, и право на обслуживание переходит к очереди с более низким CoS. Если счетчик кредитов опускается ниже нуля, очередь не обслуживается до тех пор, пока ее кредиты не будут снова пополнены. Счетчики кредитов всех очередей CoS при достижении нуля пополняются за 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)#
```

69-12 mls qos trust

Данная команда используется для настройки доверенного статуса (Trust) на порту для поля CoS или DSCP поступающего пакета для последующих QoS-операций. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
mls qos trust {cos | dscp}
no mls qos trust
```

Параметры

cos	Укажите, чтобы назначить биты CoS поступающих пакетов доверенными для последующих QoS-операций.
dscp	Укажите, чтобы назначить биты ToS/DSCP (если доступны в поступающих пакетах) доверенными для последующих операций. Для не IP-пакетов: доверенной будет назначена информация 2 уровня CoS для классификации трафика.

По умолчанию

По умолчанию доверенным является CoS.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

После настройки статуса Trust для DSCP на интерфейсе, для последующих QoS-операций DSCP 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.

Пакет, полученный портом, будет инициализирован с цветом на основе команды **mls qos map dscp-color** (если на порту настроен статус Trust для DSCP) или с цветом на основе MLS QoS преобразованного CoS (если на порту настроен статус Trust для CoS).

Пример

В данном примере показано, как настроить режим Trust для DSCP на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)#
```

69-13 police

Данная команда используется для настройки Traffic Policing (ограничения трафика) с использованием Single Rate. Используйте форму по, чтобы оменить Traffic Policing.

police *KBPS* [*BURST-NORMAL* [*BURST-MAX*]] [**conform-action** *ACTION*] **exceed-action** *ACTION* [**violate-action** *ACTION*] [**color-aware**]**no police**

Параметры

<i>KBPS</i>	Укажите среднюю скорость в Кбит/с.
<i>BURST-NORMAL</i>	(Опционально) Укажите нормальный размер всплеска (Burst). Единица измерения – Кбайт.
<i>BURST-MAX</i>	(Опционально) Укажите максимальный размер всплеска (Burst). Единица измерения – Кбайт.
conform-action	(Опционально) Укажите, чтобы действие было выполнено к Green Color Packets (пакетам «окрашенным» в зелёный цвет). Если не указано, будет выполнено действие по умолчанию transmit (передача пакетов).
exceed-action	Укажите, чтобы действие было выполнено к Yellow Color

	Packets (пакетам, «окрашенным» в желтый цвет), превышающим разрешенную скорость.
violate-action	(Опционально) Укажите, чтобы действие было выполнено к Red Color Packets (пакетам, «окрашенным» в красный цвет). Если данный параметр не указан, используется Single Rate Two Color Policer. Если данный параметр указан, используется Single Rate Three Color Policer.
ACTION	Укажите, чтобы действие было выполнено к пакетам. Ниже указаны ключевые слова: drop – отбрасывание пакетов. set-dscp-transmit VALUE – укажите значение IP DSCP-метки и передачу пакетов с новой IP DSCP-меткой. set-1p-transmit – укажите значение 802.1p и передачу пакетов с новым значением. transmit – передача пакетов без изменений.
color-aware	(Опционально) Укажите данный параметр для Single Rate Three Color Policer. Если данный параметр не указан, Policer работает в режиме Color Blind. Если данный параметр указан, Policer работает в режиме Color Aware.

По умолчанию

Нет

Режим ввода команды

Policy-map Class Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду **police**, чтобы отбросить или отметить пакеты со значениями QoS, не соответствующими уровню пакета.

Используйте команду **police KBPS**, чтобы создать Single Rate Policer. Используйте команду **police cir**, чтобы создать Two Rate Policer. Single Rate Policer может быть Two Color Policer (если указан параметр **violate-action**) или Three Color Policer (если **violate-action** не указан).

Прибывший на порт пакет будет инициализирован с цветом. Если на получающем порту настроен статус Trust для DSCP, то начальный цвет пакета будет соответствовать входящему DSCP на основе DSCP в карте цветов. Если на получающем порту настроен статус Trust для CoS, то начальный цвет пакета будет соответствовать входящему CoS на основе CoS в карте цветов.

Настроить Single Rate Two Color Policer можно только в режиме Color Blind. В режиме Color Aware может работать как Single Rate Three Color Policer, так и Two Rate Three Color Policer. В режиме Color Blind окончательный цвет пакета определяется только результатом работы policer metering. В режиме Color Aware окончательный цвет пакета определяется начальным цветом пакета и результатом работы policer metering. В данном случае Policer может понизить начальный цвет пакета.

После завершения работы `policer metering` действие будет выполнено на основе окончательного цвета. Для Green Color Packets применяется действие **conform**, для Yellow Color Packets – действие **exceed**, а для Red Color Packets – **violate**. Действия должны быть согласованы, то есть, например, нельзя указать действие **violate** с **transmit** (передачей) или **exceed** с **drop** (отбрасыванием).

Действия, настроенные в данной команде для класса трафика, будут применены ко всем пакетам, принадлежащим к данному классу трафика.

Пример

В данном примере показано, как настроить класс трафика и критерии соответствия для политики, которую необходимо привязать к настроенному классу трафика в карте политики. Команда **service-policy** используется для привязки данной политики обслуживания к интерфейсу. Traffic Policing настроено для всех входящих пакетах на интерфейсе Ethernet 1/0/1. Настроенная средняя скорость – 8 Кбит/с. Нормальный размер всплеска – 1 Кбайт.

```
Switch# configure terminal
Switch(config)# class-map access-match
Switch(config-cmap)# match access-group name acl_rd
Switch(config-cmap)# exit
Switch(config)# policy-map police-setting
Switch(config-pmap)# class access-match
Switch(config-pmap-c)# police 8 1 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# service-policy input police-setting
Switch(config-if)#
```

69-14 police aggregate

Данная команда используется для настройки Aggregate Policer в качестве политики для класса трафика в карте политик. Используйте форму **no**, чтобы удалить Aggregate Policer из политики класса.

police aggregate *NAME*
no police

Параметры

<i>NAME</i>	Укажите ранее настроенное имя Aggregate Policer в качестве Aggregate Policer для класса трафика.
-------------	--

По умолчанию

Нет

Режим ввода команды

Policy-map Class Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду **mls qos aggregate-policer** в режиме Global Configuration Mode, чтобы создать Aggregate Policer. Затем используйте команду **police aggregate** в режиме Policy-map Class Configuration Mode, чтобы настроить Aggregate Policer в качестве политики для класса трафика. Для разных карт политики настройка общего Aggregate Policer невозможна. Если именованный Aggregate Policer привязан к нескольким входным портам, работа функции Metering будет применена только к трафику, полученному на определенном порту.

Пример

В данном примере показано, как настроить параметры Aggregate Policer и применить его к нескольким классам в карте политики. Имя Aggregate Policer – `agg_policer1`. Данный Policer создан с использованием Single Rate Policing и настроен в качестве политики для класса трафика 1, 2 и 3.

```
Switch# configure terminal
Switch(config)# mls qos aggregate-policer agg_policer1 10000 16384 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)#
```

69-15 police cir

Данная команда используется для настройки Two-Rate Traffic Policing (CIR и PIR). Используйте форму **no**, чтобы отменить Two-Rate Traffic Policing.

police cir *CIR* [**bc** *CONFORM-BURST*] **pir** *PIR* [**be** *PEAK-BURST*] [**conform-action** *ACTION*][**exceed-action** *ACTION*] [**violate-action** *ACTION*] [**color-aware**]
no police

Параметры

<i>CIR</i>	Укажите гарантированную полосу пропускания (Committed Information Rate) в Кбит/с. Данный параметр является первым в алгоритме «корзина маркеров» (Token Bucket) для Two-rate Metering.
<i>PIR</i>	Укажите пиковую скорость передачи (Peak Information Rate) в Кбит/с. Данный параметр является вторым в алгоритме «корзина маркеров» (Token Bucket) для Two-rate Metering.
<i>CONFORM-BURST</i>	(Опционально) Укажите размер всплеска (Burst) для первого параметра алгоритма «корзина маркеров» (Token Bucket). Единица измерения – Кбайт.
<i>PEAK-BURST</i>	(Опционально) Укажите размер всплеска (Burst) для второго параметра алгоритма «корзина маркеров» (Token Bucket). Единица измерения – Кбайт.

conform-action	(Опционально) Укажите, чтобы действие было выполнено к Green Color Packets (пакетам, «окрашенным» в зелёный цвет). Если не указано, будет выполнено действие по умолчанию transmit (передача пакетов).
exceed-action	(Опционально) Укажите, чтобы действие было выполнено к Yellow Color Packets (пакетам, «окрашенным» в желтый цвет), которые соответствуют PIR, но не соответствуют CIR. Если не указано, будет выполнено действие по умолчанию drop (отбрасывание).
violate-action	(Опционально) Укажите, чтобы действие было выполнено к Red Color Packets (пакетам, «окрашенным» в красный цвет), которые не соответствуют CIR и PIR. Если не указано, будет выполнено действие по умолчанию drop (отбрасывание).
ACTION	(Опционально) Укажите, чтобы действие было выполнено к пакетам. Ниже указаны ключевые слова: drop – отбрасывание пакетов. set-dscp-transmit VALUE – укажите значение IP DSCP-метки и передачу пакетов с новой IP DSCP-меткой. set-1p-transmit – укажите значение 802.1p и передачу пакетов с новым значением. transmit – передача пакетов без изменений.
color-aware	(Опционально) Укажите данный параметр для Two Rate Three Color Policer. Если данный параметр не указан, Policer работает в режиме Color Blind. Если данный параметр указан, Policer работает в режиме Color Aware.

По умолчанию

Нет

Режим ввода команды

Policy-map Class Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Прибывший на порт пакет будет инициализирован с цветом. Начальный цвет пакета будет определен в соответствии с DSCP входящего пакета (если на получающем порту настроен статус Trust для DSCP) или в соответствии с CoS входящего пакета (если на получающем порту настроен статус Trust для CoS).

Single Rate Three Color Policer и Two Rate Three Color Policer могут работать в режиме Color Aware. В режиме Color Blind окончательный цвет пакета определяется только результатом работы policer metering. В режиме Color Aware окончательный цвет пакета определяется начальным цветом пакета и результатом работы policer metering. В данном случае Policer может понизить начальный цвет пакета.

После завершения работы policer metering действие будет выполнено на основе окончательного цвета. Для Green Color Packets применяется действие **conform**, для Yellow Color Packets – действие **exceed**, а для Red

Color Packets – **violate**. Действия должны быть согласованы, то есть, например, нельзя указать действие **violate** с **transmit** (передача) или **exceed** с **drop** (отбрасыванием).

Действия, настроенные в данной команде для класса трафика, будут применены ко всем пакетам, принадлежащим к данному классу трафика.

Пример

В данном примере показано, как настроить Two-Rate Traffic Policing для класса «police». Для ограничения трафика настроены средняя согласованная скорость 500 Кбит/с и пиковая скорость передачи 1 Мбит/с. Карта политики под именем «policy1» привязана к интерфейсу Ethernet 1/0/3.

```
Switch# configure terminal
Switch(config)# class-map police
Switch(config-cmap)# match access-group name myAcl101
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class police
Switch(config-pmap-c)# police cir 500 bc 10 pir 1000 be 10 exceed-action set-dscp-transmit 2
violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# service-policy output policy1
Switch(config-if)#
```

69-16 policy-map

Данная команда используется для входа в режим Policy-map Configuration Mode и создания/изменения карты политики, которая может быть привязана к одному или нескольким интерфейсам в качестве политики обслуживания. Используйте форму **no**, чтобы удалить карту политики.

policy-map *NAME*
no policy-map *NAME*

Параметры

<i>NAME</i>	Укажите имя карты политики. Максимально допустимое количество символов – 32.
-------------	--

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы войти в режим Policy-map Configuration Mode и настроить/изменить политику для класса трафика. Одна карта политики может быть привязана к нескольким интерфейсам одновременно. Предыдущие привязки карты политики будут перезаписаны новыми.

Карты политики содержат классы трафика, которые включают в себя одну или более команд для соответствия пакетов и для организации пакетов в группы на основе типа протокола или приложения.

Пример

В данном примере показано, как создать карту политики под именем «policy» и настроить для нее две политики класса. Первый класс «class1» указывает политику для трафика, соответствующего списку управления доступом (ACL) «acl_rd». Второй класс является классом по умолчанию «class-default». В данный класс включены пакеты, которые не соответствуют настроенным классам.

```
Switch# configure terminal
Switch(config)# class-map class1
Switch(config-cmap)# match access-group name acl_rd
Switch(config-cmap)# exit
Switch(config)# policy-map policy
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 46
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set ip dscp 00
Switch(config-pmap-c)#
```

69-17 priority-queue cos-map

Данная команда используется для привязки CoS к карте очереди. Используйте форму по, 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Полученному пакету присваивается внутренний CoS, который используется для выбора очереди передачи на основе привязки карты CoS к карте очереди. Чем выше значение CoS очереди, тем выше приоритет.

Пример

В данном примере показано, как привязать приоритет CoS 3, 5 и 6 к очереди 2.

```
Switch# configure terminal
Switch(config)# priority-queue cos-map 2 3 5 6
Switch(config)#
```

69-18 queue rate-limit

Данная команда используется для указания/изменения полосы пропускания (Bandwidth), предназначенной для очереди. Используйте форму **no**, чтобы удалить полосу пропускания, предназначенную для очереди.

```
queue QUEUE-ID rate-limit {MIN-BANDWIDTH-KBPS | percent MIN-PERCENTAGE} {MAX-BANDWIDTH-KBPS | percent MAX PERCENTAGE}
no queue QUEUE-ID rate-limit
```

Параметры

<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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить минимальную и максимальную полосу пропускания для определенной очереди. Если минимальная полоса пропускания настроена, пакет, передаваемый из данной

очереди, гарантирован. Если настроена максимальная полоса пропускания, пакеты, передаваемые из данной очереди, не могут превышать максимальную полосу пропускания, даже если полоса пропускания доступна.

Значение всей минимальной полосы пропускания должно быть меньше 75 процентов полосы пропускания интерфейса. Для очереди с наивысшим приоритетом настройка минимальной разрешенной полосы пропускания необязательна, так как трафик данной очереди обслуживается в первую очередь, если все очереди соответствуют заданной минимальной полосе пропускания.

Данная команда используется для настройки физического порта, для `port-channel` команда недоступна. На физических портах невозможна настройка минимальной разрешенной полосы пропускания одного CoS.

Пример

В данном примере показано, как настроить полосу пропускания очереди для интерфейса Ethernet 1/0/1. Для очереди 1 «queue 1» настроены минимальная разрешенная полоса пропускания 100 Кбит/с и максимальная полоса пропускания 2000 Кбит/с. Для очереди 2 «queue 2» настроены минимальная разрешенная полоса пропускания 10% и максимальная полоса пропускания 50%.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# queue 1 rate-limit 100 2000
Switch(config-if)# queue 2 rate-limit percent 10 percent 50
Switch(config-if)#
```

69-19 rate-limit {input | output}

Данная команда используется для настройки значений ограничения полосы пропускания для входящего и исходящего трафика на интерфейсе. Используйте форму **no**, чтобы отменить ограничение полосы пропускания.

rate-limit {input | output} {NUMBER-KBPS | percent PERCENTAGE} [BURST-SIZE]
no rate-limit {input | output}

Параметры

input	Укажите ограничение полосы пропускания для входящих пакетов.
output	Укажите ограничение полосы пропускания для исходящих пакетов.
<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

Уровень команды по умолчанию

Уровень 12

Использование команды

Настроенное ограничение не должно превышать максимальную скорость на указанном интерфейсе. Если полученный трафик превышает настроенное ограничение входящей полосы пропускания, отправляются кадры PAUSE или кадры Flow Control (управления потоком).

Пример

В данном примере показано, как настроить ограничения максимальной полосы пропускания на интерфейсе Ethernet 1/0/5. Настроенные ограничения входящей полосы пропускания: 2000 Кбит/с и 4096 Кбайт для трафика всплеска (Burst).

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/5
Switch(config-if)# rate-limit input 2000 4096
Switch(config-if)#
```

69-20 service-policy

Данная команда используется для привязки карты политики к типу input или output на интерфейсе. Используйте форму **no**, чтобы удалить политику обслуживания из входящего интерфейса (input).

service-policy {input | output} NAME
no service-policy {input | output}

Параметры

input	Укажите, чтобы привязать карту политики к входящему потоку на интерфейсе.
output	Укажите, чтобы привязать карту политики к исходящему потоку на интерфейсе.
<i>NAME</i>	Укажите имя карты политики обслуживания. Максимально допустимое количество символов – 32.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы привязать карту политики к типу input или output на интерфейсе. К каждому типу (input или output) может быть привязана только одна карта политики. Политика, привязанная к интерфейсу, позволяет объединять и контролировать число или скорость пакетов. Поступающий на порт пакет будет обработан на основе политики обслуживания, привязанной к данному интерфейсу.

Пример

В данном примере показано, как настроить две карты политики: (1) cust1-classes и (2) cust2-classes. Для cust1-classes: карта класса «gold» настроена для привязки CoS 6 с использованием Single Rate Policer, настроенная согласованная скорость передачи – 800 Кбит/с; карта класса «silver» настроена для привязки CoS 5 с использованием Single Rate Policer, настроенная согласованная скорость передачи – 2000 Кбит/с; карта класса «bronze» настроена для привязки CoS 0 с использованием Single Rate Policer, настроенная согласованная скорость передачи – 8000 Кбит/с.

Для cust2-classes: карта класса «gold» настроена с использованием очереди CoS 6 и Single Rate Policer, настроенная согласованная скорость передачи – 1600 Кбит/с; карта класса «silver» настроена с использованием Single Rate Policer, настроенная согласованная скорость передачи – 4000 Кбит/с; карта класса «bronze» настроена с использованием Single Rate Policer, настроенная согласованная скорость передачи – 16000 Кбит/с.

Настроенная карта политики «cust1-classes» привязана к интерфейсам Ethernet 1/0/1 и 1/0/2 для входящего трафика.

```
Switch# configure terminal
Switch(config)# class-map match-all gold
Switch(config-cmap)# match cos 6
Switch(config-cmap)# exit
Switch(config)# class-map match-all silver
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
Switch(config)# class-map match-all bronze
Switch(config-cmap)# match cos 0
Switch(config-cmap)# exit
Switch(config)# policy-map cust1-classes
Switch(config-pmap)# class gold
Switch(config-pmap-c)# police 800 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver
Switch(config-pmap-c)# police 2000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze
Switch(config-pmap-c)# police 8000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# service-policy input cust1-classes
Switch(config-if)# exit
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# service-policy input cust1-classes
Switch(config-if)#
```

Настроенная карта политики «cust2-classes» привязана к интерфейсу Ethernet 1/0/1 для входящего трафика.


```

Switch# configure terminal
Switch(config)# policy-map cust2-classes
Switch(config-pmap)# class gold
Switch(config-pmap-c)# police 1600 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver
Switch(config-pmap-c)# police 4000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze
Switch(config-pmap-c)# police 16000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# service-policy input cust2-classes
Switch(config-if)#

```

69-21 set

Данная команда используется для настройки полей нового приоритета (Precedence), DSCP и CoS исходящего пакета. Также возможна настройка очереди CoS для пакета.

```

set {[ip] precedence PRECEDENCE | [ip] dscp DSCP | cos COS | cos-queue COS-QUEUE}
no set {[ip] precedence PRECEDENCE | [ip] dscp DSCP | cos COS | cos-queue COS-QUEUE}

```

Параметры

precedence <i>PRECEDENCE</i>	Укажите новый приоритет пакета. Доступный диапазон значений: от 0 до 7. Если указано ключевое слово ip , будет отмечен приоритет IPv4. Если не указано, будут отмечены приоритеты IPv4 и IPv6. Для пакетов IPv6 приоритетом являются три наиболее значимых бита класса трафика заголовка IPv6. Настройка приоритета не повлияет на выбор очереди CoS.
dscp <i>DSCP</i>	Укажите новый DSCP пакета. Доступный диапазон значений: от 0 до 63. Если указано ключевое слово ip , будет отмечен IPv4 DSCP. Если не указано, будут отмечены IPv4 и IPv6 DSCP. Настройка DSCP не повлияет на выбор очереди CoS.
cos <i>COS</i>	Укажите новое значение CoS пакета. Доступный диапазон значений: от 0 до 7. Настройка CoS не повлияет на выбор очереди CoS.
cos-queue <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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить новое значение полей приоритета (Precedence), DSCP и CoS соответствующих пакетов. Используйте команду **set cos-queue**, чтобы сразу же назначить очередь CoS для соответствующих пакетов.

Возможна настройка нескольких команд для класса, если они не конфликтуют.

Команда **set dscp** не повлияет на выбор очереди CoS. Команда **set cos-queue** не изменит поле CoS исходящего пакета. Команды **police** и **set** могут быть использованы для одного класса. Команда **set** применяется к пакетам всех цветов.

Пример

В данном примере показано, как настроить карту политики «policy1» для класса «class1». Пакеты в настроенном классе «class1» будут помечены DSCP 10 с использованием Single Rate Policer, настроенная согласованная скорость передачи – 1 Мбит/с.

```
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap-c)# police 1000000 2000 exceed-action set-dscp-transmit 10
Switch(config-pmap-c)# exit
Switch(config-pmap)#
```

69-22 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

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить все карты класса и их критерии соответствия.

Пример

В данном примере показано, как настроены две карты класса. Пакеты, соответствующие списку доступа «acl_home_user», принадлежат настроенному классу «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#
```

69-23 show mls qos aggregate-policer

Данная команда используется для отображения настроенного Aggregated Policer.

show mls qos aggregate-policer [NAME]

Параметры

<i>NAME</i>	(Опционально) Укажите имя Aggregated Policer.
-------------	---

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить настроенный Aggregated Policer.

Пример

В данном примере показано, как отобразить Aggregated Policer.

```
Switch# show mls qos aggregate-policer

mls qos aggregate-policer agg-policer5 10 1000 conform-action transmit exceed-action drop
mls qos aggregate-policer agg-policer5 cir 500 bc 10 pir 1000 be 10 conform-action transmit
exceed-action set-dscp-transmit 2 violate-action drop

Switch#
```

69-24 show mls qos interface

Данная команда используется для отображения настроек уровня QoS на указанном интерфейсе.

show mls qos interface *INTERFACE-ID* [, | -] {**cos** | **scheduler** | **trust** | **rate-limit** | **queue-rate-limit** | **dscp-mutation** | **map** {**dscp-color** | **cos-color** | **dscp-cos**}}

Параметры

interface <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.
cos	Укажите, чтобы отобразить CoS по умолчанию.
scheduler	Укажите, чтобы отобразить настройки механизма обслуживания очереди передачи.
trust	Укажите, чтобы отобразить статус Trust порта.
rate-limit	Укажите, чтобы отобразить ограничение полосы пропускания, настроенной для порта.
queue-rate-limit	Укажите, чтобы отобразить ограничение полосы пропускания, настроенной для очереди.
dscp-mutation	Укажите, чтобы отобразить карту DSCP Mutation, привязанную к интерфейсу.
map dscp-color	Укажите, чтобы отобразить цветовую привязку DSCP.
map cos-color	Укажите, чтобы отобразить цветовую привязку CoS.
map dscp-cos	Укажите, чтобы отобразить привязку DSCP к CoS.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения настроек уровня QoS на указанном интерфейсе.

Пример

В данном примере показано, как отобразить CoS по умолчанию для интерфейсов от Ethernet 1/0/2 до Ethernet 1/0/5.

```
Switch# show mls qos interface ethernet 1/0/2-5 cos
```

Interface	CoS	Override
eth1/0/2	3	Yes
eth1/0/3	4	No
eth1/0/4	4	No
eth1/0/5	3	No

```
Switch#
```

В данном примере показано, как отобразить статус Trust порта для интерфейсов от Ethernet 1/0/2 до Ethernet 1/0/5.

```
Switch# show mls qos interface ethernet 1/0/2-1/0/5 trust
```

Interface	Trust State
eth1/0/2	trust DSCP
eth1/0/3	trust CoS
eth1/0/4	trust DSCP
eth1/0/5	trust CoS

```
Switch#
```

В данном примере показано, как отобразить настройки механизма обслуживания очередей для интерфейсов Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch# show mls qos interface ethernet 1/0/1-1/0/2 scheduler
```

Interface	Scheduler Method
eth1/0/1	sp
eth1/0/2	wrr

```
Switch#
```

В данном примере показано, как отобразить карты DSCP Mutation, которые привязаны к интерфейсам Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch# show mls qos interface ethernet 1/0/1-2 dscp-mutation

Interface      DSCP Mutation Map
-----
eth1/0/1       Mutate Map 1
eth1/0/2       Mutate Map 2

Switch#
```

В данном примере показано, как отобразить ограничение полосы пропускания для интерфейсов от Ethernet 1/0/1 до Ethernet 1/0/4.

```
Switch# show mls qos interface ethernet 1/0/1-4 rate-limit

Interface      Rx Rate          Tx Rate          Rx Burst        Tx Burst
-----
eth1/0/1       1000 kbps        No Limit         64 kbyte        No Limit
eth1/0/2       No Limit         2000 kbps        No Limit        2000 kbyte
eth1/0/3       10%(1000000 kbps) 20%(2000000 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%(1000000 kbps)
  2     32 kbps       -
  3     2%           50%
  4     64 kbps       -
  5     64 kbps       -
  6     32 kbps       -
  7     -             128 kbps

eth1/0/2
  QID  Min Bandwidth  Max Bandwidth
  ----  -
  0     -             -
  1     16 kbps       -
  2     32 kbps       -
  3     32 kbps       -
  4     64 kbps       -
  5     64 kbps       -
  6     32 kbps       -
  7     -             128 kbps

Switch#
```

В данном примере показано, как отобразить цветовую привязку DSCP для интерфейсов Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch# show mls qos interface ethernet 1/0/1-2 map dscp-color

eth1/0/1
  DSCP 0-7 are mapped to green
  DSCP 8-40 are mapped to red
  DSCP 41-43 are mapped to yellow
eth1/0/2
  DSCP 0 - 7 are mapped to green

Switch#
```

В данном примере показано, как отобразить цветовую привязку CoS для интерфейсов Ethernet 1/0/3 и Ethernet 1/0/4.

```
Switch# show mls qos interface ethernet 1/0/3-4 map cos-color

eth1/0/3
  CoS 0,1,2 are mapped to green
  CoS 3-4 are mapped to yellow
  CoS 6 are mapped to red
eth1/0/4
  CoS 0,1-6 are mapped to green

Switch#
```

В данном примере показано, как отобразить привязку DSCP к CoS для интерфейса Ethernet 1/0/1.

```
Switch# show mls qos interface ethernet 1/0/1 map dscp-cos

eth1/0/1
0  1  2  3  4  5  6  7  8  9
-----
00  00 00 00 00 00 00 00 00 01 01
10  01 01 01 01 01 01 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#
```

69-25 show mls qos map dscp-mutation

Данная команда используется для отображения настроек карты QoS DSCP Mutation.

```
show mls qos maps dscp-mutation [MAP-NAME]
```

Параметры

MAP-NAME (Опционально) Укажите имя карты DSCP Mutation, которую необходимо отобразить.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения настроек карты QoS DSCP Mutation.

Пример

В данном примере показано, как отобразить карту DSCP Mutation глобально.

```
Switch#show mls qos map dscp-mutation

DSCP Mutation: mutation
Attaching interface:
  eth1/0/2-1/0/3,1/0/8-1/0/10

  0  1  2  3  4  5  6  7  8  9
  -----
00  00 10 02 10 04 05 06 07 08 09
10  10 11 12 13 14 15 16 17 18 19
20  20 21 22 23 24 25 26 27 28 29
30  30 31 32 33 34 35 36 37 38 39
40  40 41 42 43 44 45 46 47 48 49
50  50 51 52 53 54 55 56 57 58 59
60  60 61 62 63

Switch#
```

69-26 show mls qos queueing

Данная команда используется для отображения информации об очередях QoS и настроек веса (Weight) для разных алгоритмов обслуживания очередей на определенном интерфейсе или интерфейсах.

show mls qos queueing [interface INTERFACE-ID [, | -]]

Параметры

interface <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

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

При указании ключевого слова **interface**, на определенном интерфейсе или интерфейсах будет отображен настроенный вес для разных алгоритмов обслуживания очередей (WRR или WDRR). Если **interface** не указан, отображается только системная карта привязки CoS к ID очереди.

Режим Scheduling, который настроен при помощи команды **mls qos scheduler**, определяет, какие настройки будут действовать для веса. Используйте команду **show mls qos interface scheduler**, чтобы отобразить настроенный алгоритм обслуживания очередей на интерфейсе.

Пример

В данном примере показано, как отобразить информацию об очередях QoS.

```
Switch#show mls qos queueing
```

```
CoS-queue map:
```

```
CoS  QID
```

```
---  ---
```

```
0    2
```

```
1    0
```

```
2    1
```

```
3    3
```

```
4    4
```

```
5    5
```

```
6    6
```

```
7    7
```

```
Switch#
```

В данном примере показано, как отобразить настройки веса для разных алгоритмов обслуживания очередей на интерфейсе Ethernet 1/0/3.

```
Switch#show mls qos queueing interface ethernet 1/0/3

Interface: eth1/0/3
wrr bandwidth weights:
  QID  Weights
  ---  -
  0    1
  1    1
  2    1
  3    1
  4    1
  5    1
  6    1
  7    0

wdrp bandwidth weights:
  QID  Quantum
  ---  -
  0    1
  1    1
  2    1
  3    1
  4    1
  5    1
  6    1
  7    1

Switch#
```

69-27 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.
interface <i>INTERFACE-ID</i>	(Опционально) Укажите модуль и номер порта.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить политики класса, настроенные для карты политики. Также команда используется для отображения настроек политики класса определенных или всех существующих карт политики обслуживания.

Пример

В данном примере показано, как настроить Two-Rate Traffic Policing в карте политики под именем «policy1» для класса «police». Для ограничения трафика настроены средняя согласованная скорость 500 Кбит/с и пиковая скорость передачи 1 Мбит/с.

```
Switch# configure terminal
Switch(config)# class-map police
Switch(config-cmap)# match access-group name acl_rd
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class police
Switch(config-pmap-c)# police cir 500 bc 10 pir 1000 be 10 exceed-action set-dscp-transmit 2
violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface ethernet 1/0/1
Router(config-if)# service-policy output policy1
Router(config-if)#
```

В данном примере показано, как отобразить карту политики, настроенную в примере выше. Имя настроенной карты политики – policy1.

```
Switch#show policy-map policy1

Policy Map policy1
  Class Map police
police cir 500 bc 10 pir 1000 be 10 conform-action transmit exceed-action set-dscp-transmit 2
violate-action drop

Switch#
```

В данном примере показано, как отобразить все карты политики на интерфейсе Ethernet 1/0/1.

```
Switch#show policy-map interface ethernet 1/0/1

Policy Map: policy1 : output
  Class Map police
police cir 500 bc 10 pir 1000 be 10 conform-action transmit exceed-action set-dscp-transmit 2
violate-action drop

Switch#
```

69-28 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>	Укажите значение Quantum (число длины кадров) для каждой очереди, обслуживаемой механизмом WDRR.
----------------------------	--

По умолчанию

Значение Quantum для каждой очереди по умолчанию – 1.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Чтобы использовать данную команду, необходимо перейти в режим обслуживания очередей WDRR с помощью команды **mls qos scheduler 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 ethernet 1/0/1
Switch(config-if)# mls qos scheduler wdr
Switch(config-if)# wdr-queue bandwidth 1 2 3 4 5 6 7 8
Switch(config-if)#
```

69-29 wrr-queue bandwidth

Данная команда используется для настройки веса (Weight) для очередей, обслуживаемых механизмом WRR. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

wrr-queue bandwidth WEIGHT1...WEIGHT8
no wrr-queue bandwidth

Параметры

<i>WEIGHT1...WEIGHT8</i>	Укажите значение веса (число кадров) для каждой очереди, обслуживаемой механизмом WRR.
--------------------------	--

По умолчанию

Значение веса для параметров от *WEIGHT1* до *WEIGHT7* по умолчанию – 1.
Значение веса для *WEIGHT8* по умолчанию – 0.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Чтобы использовать данную команду, необходимо перейти в режим обслуживания очередей WRR с помощью команды **mls qos scheduler wrr**. При обслуживании Expedited Forwarding (EF) для очереди с наивысшим приоритетом всегда используется политика Per-hop Behavior (PHB) EF и настраивается режим обслуживания очередей по строгому приоритету (Strict Priority). При использовании Differentiate Service необходимо, чтобы вес последней очереди был равен нулю.

Пример

В данном примере показано, как настроить значения веса (Weight) очередей в режиме обслуживания очередей WRR на интерфейсе Ethernet 1/0/1. Для очереди 0 настроено значение 1, для очереди 1 – 2, для очереди 2 – 3, для очереди 3 – 4, для очереди 5 – 6, для очереди 6 – 7 и для очереди 7 – 8.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# mls qos scheduler wrr
Switch(config-if)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
Switch(config-if)#
```

70. Команды перезагрузки

70-1 reboot

Данная команда используется для перезагрузки коммутатора.

reboot [force_agree]

Параметры

force_agree	(Опционально) Укажите, чтобы перезагрузить коммутатор без дополнительного подтверждения.
--------------------	--

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Данная команда используется для перезагрузки коммутатора.

Пример

В данном примере показано, как перезагрузить коммутатор.

```
Switch# reboot force_agree
Please wait, the switch is rebooting...
```

70-2 reboot schedule

Данная команда используется для настройки расписания перезагрузки. Используйте форму **no**, чтобы отменить расписание перезагрузки.

reboot schedule {in MINUTES | at HH:MM [DDMTHYYYY]} [save_before_reboot]
no reboot schedule

Параметры

in MINUTES	Укажите период времени, по истечении которого будет выполнена перезагрузка коммутатора. Доступный диапазон значений: от 1 до 43200 минут.
-------------------	---

at	Укажите точную дату и время для перезагрузки коммутатора. Запланированная перезагрузка должна быть выполнена в течение 30 дней.
<i>HH:MM</i>	Укажите время перезагрузки коммутатора.
<i>DDMMTHYYYY</i>	(Опционально) Введите дату перезагрузки коммутатора. Если дата не указана, перезагрузка будет выполнена в указанное время текущего дня. Если указанное время прошло, перезагрузка выполняется на следующий день.
save_before_reboot	Укажите, чтобы сохранить все настройки перед перезагрузкой коммутатора.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить расписание перезагрузки. После перезагрузки коммутатора в журнале появится сообщение о том, что система была перезагружена при помощи команды **reboot schedule**.

Расписание перезагрузки не сохраняется в файле конфигурации и удаляется автоматически после перезагрузки или отключения коммутатора. Также указанное расписание перезагрузки отменяется, если коммутатор был отключен или перезагружен вручную перед применением данного расписания.

Пример

В данном примере показано, как сохранить настройки перед перезагрузкой коммутатора, которая будет выполнена через 10 минут.

```
Switch# reboot schedule in 10 save_before_reboot
Switch#
```

В данном примере показано, как настроить перезагрузку на 23:00, 27 марта 2015 г.

```
Switch# reboot schedule at 23:00 27mar2015
Switch#
```

70-3 show reboot schedule

Данная команда используется для отображения настроек расписания перезагрузки.

show reboot schedule

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения настроек расписания перезагрузки.

Пример

В данном примере показано, как отобразить настройки расписания перезагрузки.

```
Switch#show reboot schedule

Reboot Schedule Settings
-----
Reboot schedule at 27 Mar 2015 23:00:00 (in 520 minutes)
Save before reboot: Yes

Switch#
```


71. Команды Remote Network MONitoring (RMON)

71-1 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Номер записи группы статистики RMON является динамическим. Соответствующая запись в таблице будет доступна только на интерфейсе с включенной статистикой RMON.

Пример

В данном примере показано, как настроить запись статистики RMON на интерфейсе Ethernet 1/0/2. Индекс – 65. Имя владельца – guest.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# rmon collection stats 65 owner guest
Switch(config-if)#
```

71-2 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.
owner NAME	Укажите имя владельца. Максимально допустимое количество символов в строке – 127.
buckets NUM	Укажите количество ячеек для сбора истории по группе статистики RMON. Доступный диапазон значений: от 1 до 65535. Если не указано, используется значение по умолчанию – 50.
interval SECONDS	Укажите время в секундах для каждого цикла опроса (Polling Cycle). Доступный диапазон значений: от 1 до 3600.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Номер записи группы статистики RMON является динамическим. Соответствующая запись в таблице будет доступна только на интерфейсе с включенной статистикой RMON. Настроенный интерфейс становится источником данных для созданной записи.

Пример

В данном примере показано, как включить сбор истории по группе статистики RMON MIB на интерфейсе Ethernet 1/0/8.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/8
Switch(config-if)# rmon collection history 101 owner it@domain.com interval 2000
Switch(config-if)#
```

71-3 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

<i>INDEX</i>	Укажите индекс alarm. Доступный диапазон значений: от 1 до 65535.
<i>VARIABLE</i>	Укажите идентификатор объекта переменной для выборки.
<i>INTERVAL</i>	Укажите интервал в секундах для выборки переменной и проверки соответствия пороговых значений. Доступный диапазон значений: от 1 до 2147483647.
delta	Укажите для мониторинга дельты (Delta) двух последовательных значений выборки.
absolute	Укажите для мониторинга абсолютного значения выборки
rising-threshold VALUE	Укажите верхнее пороговое значение. Доступный диапазон значений: от 0 до 2147483647.
<i>RISING-EVENT-NUMBER</i>	(Опционально) Укажите индекс записи события, при котором превышено заданное верхнее пороговое значение. Доступный диапазон значений: от 1 до 65535. Если не указано, никакие действия при превышении верхнего порогового значения не будут применены.
falling-threshold VALUE	Укажите нижнее пороговое значение. Доступный диапазон значений: от 0 до 2147483647.
<i>FALLING-EVENT-NUMBER</i>	(Опционально) Укажите индекс записи события, при котором достигнуто заданное нижнее пороговое значение. Доступный диапазон значений: от 1 до 65535. Если не указано, никакие действия при достижении нижнего порогового значения не будут применены.
owner STRING	(Опционально) Укажите строку владельца. Максимально допустимая длина – 127.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

После настройки RMON alarm будут периодически производиться выборки переменных, значения которых будут проверены на соответствие настроенным пороговым значениям.

Пример

В данном примере показано, как настроить запись уровня alarm для мониторинга интерфейса.

```
Switch# configure terminal
Switch(config)# rmon alarm 783 1.3.6.1.2.1.2.2.1.12.6 30 delta rising-threshold 20 1 falling-
threshold 10 1 owner Name
Switch(config)#
```

71-4 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

<i>INDEX</i>	Укажите индекс записи события. Доступный диапазон значений: от 1 до 65535.
log	(Опционально) Укажите, чтобы генерировать сообщения в системном журнале для уведомлений.
trap <i>COMMUNITY</i>	(Опционально) Укажите, чтобы генерировать сообщения SNMP trap для уведомлений. Максимально допустимая длина – 127.
owner <i>NAME</i>	Укажите имя владельца. Максимально допустимая длина – 127.
description <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

Уровень команды по умолчанию

Уровень 12

Использование команды

Если указан параметр **log**, а **trap** не указан, при возникновении события генерируется запись в журнале. Если указан параметр **trap**, а **log** не указан, при возникновении события генерируется SNMP-уведомление.

Если указаны оба параметра (**log** и **trap**), при возникновении события генерируется и запись в журнале, и SNMP-уведомление.

Пример

В данном примере показано, как настроить генерирование записи в журнале при возникновении события. Индекс – 13.

```
Switch# configure terminal
Switch(config)# rmon event 13 log owner it@domain.com description ifInNUcastPkts is too much
Switch(config)#
```

71-5 show rmon alarm

Данная команда используется для отображения конфигурации alarm.

show rmon alarm

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить таблицу RMON alarm.

Пример

В данном примере показано, как отобразить таблицу RMON alarm.

```
Switch# show rmon alarm

Alarm index 23, owned by IT
  Monitors OID: 1.3.6.1.2.1.2.2.1.10.1
  every 120 second(s)
  Taking delta samples, last value was 2500
  Rising threshold is 2000, assigned to event 12
  Falling threshold is 1100, assigned to event 12
  On startup enable rising or falling alarm

Switch#
```

71-6 show rmon events

Данная команда используется для отображения таблицы событий RMON.

show rmon events

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить таблицу событий RMON.

Пример

В данном примере показано, как отобразить таблицу событий RMON.

```
Switch# show rmon events

Event 1, owned by manager1
  Description is Errors
  Event trigger action: log & trap sent to community manager
  Last triggered time: 13:12:15, 2013-03-02

Event 2, owned by manager2
  Description is Errors
  Event trigger action: log & trap
  Last triggered time:

Switch#
```

71-7 show rmon history

Данная команда используется для отображения информации об истории статистики RMON.

show rmon history

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить историю статистики для всех настроенных записей.

Пример

В данном примере показано, как отобразить историю статистики RMON Ethernet.

```
Switch# show rmon history
Index 23, owned by Manager, Data source is eth4/0/2
Interval: 30 seconds
Requested buckets: 50, Granted buckets: 50
Sample #1
  Received octets: 303595962, Received packets: 357568
  Broadcast packets: 3289, Multicast packets: 7287
  Estimated utilization: 19
  Undersized packets: 213, Oversized packets: 24
  Fragments: 2, Jabbers: 1
  CRC alignment errors: 0, Collisions: 0
Drop events : 0
Sample #2
  Received octets: 303596354, Received packets: 357898
  Broadcast packets: 3329, Multicast packets: 7337
  Estimated utilization: 19
  Undersized packets: 213, Oversized packets: 24
  Fragments: 2, Jabbers: 1
  CRC alignment errors: 0, Collisions: 0
Drop events : 0
Switch#
```

71-8 show rmon statistics

Данная команда используется для отображения статистики RMON Ethernet.

show rmon statistics

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить статистику для всех настроенных записей.

Пример

В данном примере показано, как отобразить статистику RMON.

```
Switch# show rmon statistics

Index 32, owned by it@domain.com, Data Source is eth4/0/3
Received Octets : 234000, Received packets : 9706
Broadcast packets: 2266, Multicast packets: 192
Undersized packets: 213, Oversized packets: 24
Fragments: 2, Jabbers: 1
CRC alignment errors: 0, Collisions: 0
Drop events : 0
Packets in 64 octets: 256, Packets in 65-127 octets : 236
Packets in 128-255 octets : 129, Packets in 256-511 octets : 10
Packets in 512-1023 octets : 38, Packets in 1024-1518 octets : 2200

Switch#
```

71-9 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

rising-alarm	(Опционально) Укажите, чтобы настроить отставку trap, уведомляющих о поднятии тревоги.
falling-alarm	(Опционально) Укажите, чтобы настроить отставку trap, уведомляющих об отмене тревоги.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить/отключить отправку RMON trap.

Пример

В данном показано, как включить отправку RMON trap, уведомляющих о поднятии и об отмене тревоги.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps rmon
Switch(config)#
```

72. Команды Route Map

72-1 match interface

Данная команда используется для настройки правила соответствия маршрутов исходящим интерфейсам. Используйте форму **no**, чтобы отменить правило.

```
match interface INTERFACE-ID
no match interface
```

Параметры

<i>INTERFACE-ID</i>	Укажите исходящий интерфейс.
---------------------	------------------------------

По умолчанию

Нет

Режим ввода команды

Route-map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду в режиме Route-map Configuration Mode, чтобы настроить правило соответствия маршрутов исходящим интерфейсам.

Пример

В данном примере показано, как создать запись карты маршрутов (Route Map) с соответствием исходящему интерфейсу.

```
Switch# configure terminal
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match interface vlan 1
Switch(config-route-map)#
```

72-2 match ip address

Данная команда используется для настройки правила соответствия маршрута на основе стандартного списка доступа IP или списка IP-префиксов. Используйте форму **no**, чтобы отменить правило.

```
match ip address {ACCESS-LIST-NAME}
no match ip address {ACCESS-LIST-NAME}
```

Параметры

<i>ACCESS-LIST-NAME</i>	Укажите имя стандартного или расширенного списка
-------------------------	--

 доступа IP.

По умолчанию

Нет

Режим ввода команды

Route-map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду в режиме Route-map Configuration Mode, чтобы настроить правило соответствия маршрутов списку доступа IP.

Пример

В данном примере показано, как создать список доступа IP и запись карты маршрутов с соответствием созданному списку доступа IP. Настроенный список доступа IP – myacl.

```
Switch# configure terminal
Switch(config)# ip access-list myacl
Switch(config-ip-acl)# permit 10.20.0.0 0.0.255.255 any
Switch(config-ip-acl)# exit
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match ip address myacl
Switch(config-route-map)#
```

72-3 match ip next-hop

Данная команда используется для настройки правила соответствия маршрутов следующему узлу (Next Hop) на основе стандартного списка доступа IP или списка IP-префиксов. Используйте форму **no**, чтобы отменить правило.

```
match ip next-hop {ACCESS-LIST-NAME}
no match ip next-hop {ACCESS-LIST-NAME}
```

Параметры

<i>ACCESS-LIST-NAME</i>	Укажите имя списка доступа IP.
-------------------------	--------------------------------

По умолчанию

Нет

Режим ввода команды

Route-map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду в режиме Route-map Configuration Mode, чтобы настроить правило соответствия маршрутов следующему узлу, IP-адрес которого будет проверен в соответствии со стандартным списком доступа IP или списком IP-префиксов.

Пример

В данном примере показано, как создать список доступа IP и запись карты маршрутов с соответствием следующему узлу на основе созданного списка доступа IP. Настроенный список доступа IP – myacl.

```
Switch# configure terminal
Switch(config)# ip access-list myacl
Switch(config-ip-acl)# permit 10.20.0.0 0.0.255.255
Switch(config-ip-acl)# exit
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match ip next-hop myacl
Switch(config-route-map)#
```

72-4 match ip route-source

Данная команда используется для настройки правила соответствия маршрутов IP-адресу исходного маршрутизатора на основе стандартного списка доступа IP. Используйте форму **no**, чтобы отменить правило.

match ip route-source *ACCESS-LIST-NAME*
no match ip route-source

Параметры

<i>ACCESS-LIST-NAME</i>	Укажите имя стандартного списка доступа IP.
-------------------------	---

По умолчанию

Нет

Режим ввода команды

Route-map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду в режиме Route-map Configuration Mode, чтобы настроить правило соответствия маршрутов исходному маршрутизатору, IP-адрес которого будет проверен в соответствии со стандартным списком доступа IP.

Пример

В данном примере показано, как создать список доступа IP и запись карты маршрутов с соответствием исходному маршрутизатору на основе созданного списка доступа IP. Настроенный список доступа IP – myacl.

```
Switch# configure terminal
Switch(config)# ip access-list myacl
Switch(config-ip-acl)# permit 10.20.0.0 0.0.255.255
Switch(config-ip-acl)# exit
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match ip route-source myacl
Switch(config-route-map)#
```

72-5 match metric

Данная команда используется для настройки правила соответствия метрики (Metric) маршрутов. Используйте форму **no**, чтобы отменить правило.

```
match metric VALUE
no match metric
```

Параметры

<i>VALUE</i>	Укажите метрику маршрута в диапазоне от 0 до 4294967294.
--------------	--

По умолчанию

Нет

Режим ввода команды

Route-map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду в режиме Route-map Configuration Mode, чтобы настроить правило соответствия метрики маршрутов.

Пример

В данном примере показано, как создать запись карты маршрутов с соответствием метрике маршрутов.

```
Switch# configure terminal
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match metric 10
Switch(config-route-map)#
```

72-6 route map

Данная команда используется для создания записи правила карты маршрутов (Route Map). Используйте форму **no**, чтобы удалить запись правила карты маршрутов.

```
route-map MAP-NAME {permit | deny} SEQ-NUMBER
no route-map MAP-NAME {permit | deny} SEQ-NUMBER
```

Параметры

<i>MAP-NAME</i>	Укажите имя карты маршрутов.
permit	Укажите, чтобы разрешить маршруты, соответствующие записи правила.
deny	Укажите, чтобы заблокировать маршруты, соответствующие записи правила.
<i>SEQ-NUMBER</i>	Укажите порядковый номер записи карты маршрутов. Доступный диапазон значений: от 1 до 65535.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Возможна настройка нескольких записей карты маршрутов, которые могут быть записи разрешения (permit) или запрета (deny). Если маршрут соответствует карте маршрутов, запись в карте маршрутов проверяется на соответствие маршруту на основе порядкового номера в карте маршрутов. Если запись соответствует, то к записи будет применено действие без проверки других записей карты маршрута.

Запись карты маршрутов может содержать несколько условий соответствий. Маршрут соответствует записи, если все условия соответствия были выполнены. После проверки записи будут применяться все установленные действия правила, если указано **permit**. При указании **deny** маршрут будет заблокирован.

Пример

В данном примере показано, как создать запись правила. Порядковый номер – 1. Карта маршрутов – myPolicy.

```
Switch# configure terminal
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)#
```

72-7 show route-map

Данная команда используется для отображения информации о карте маршрутов.

```
show route-map [ROUTE-MAP-NAME]
```

Параметры

<i>ROUTE-MAP-NAME</i>	(Опционально) Укажите карту маршрутов, которую необходимо отобразить.
-----------------------	---

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию о карте маршрута.

Пример

В данном примере показано, как отобразить информацию о карте маршрута.

```
Switch# show route-map
Route Map nypolicy, permit, sequence 1
  Match clauses:
    ip address myacl
  Set clauses:
    next-hop 100.1.1.1
Total Entries: 1
Total Route Map Counts : 1
Switch#
```

72-8 set ip default next-hop

Данная команда используется для настройки на маршрутизаторе следующего узла по умолчанию (Default Next Hop) для маршрутизации пакетов, которые соответствуют настроенным правилам последовательностей карты маршрутов. Используйте форму **no**, чтобы удалить определенные следующие узлы по умолчанию.

```
set ip default next-hop IP-ADDRESS [...IP-ADDRESS]
no set ip default next-hop IP-ADDRESS [...IP-ADDRESS]
```

Параметры

<i>IP-ADDRESS</i>	Укажите IP-адрес следующего узла по умолчанию для
-------------------	---

 маршрутизации пакетов.

По умолчанию

Нет

Режим ввода команды

Route-map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

На маршрутизаторе возможна настройка нескольких Default Next Hop. Если Default Next Hop уже были настроены, новые настроенные Default Next Hop будут добавлены в список ранее настроенных узлов. Если первый указанный следующий Default Next Hop на маршрутизаторе отключен, для маршрутизации пакетов будет выбран второй указанный Default Next Hop.

Пример

В данном примере показан процесс настройки политики PBR, с помощью которой пакеты будут отправлены на следующий узел (Next Hop) 120.1.2.2. IP-адрес источника – 10.1.1.0/24. Принимающий интерфейс – VLAN 100. Сначала создается основной список доступа IP, разрешающий префикс 10.1.1.0/24. Созданный список – Strict-Control. Затем создается карта маршрутов, соответствующая IP-адресу из списка префиксов созданного списка «Strict-Control». Созданная карта маршрутов – myPolicy. Для использования карты маршрутов «myPolicy» необходимо задать IP-адрес политики PBR в режиме VLAN Interface Configuration Mode.

```
Switch# configure terminal
Switch(config)# ip access-list Strict-Control
Switch(config-ip-acl)# permit 10.1.1.0 0.0.0.255 any
Switch(config-ip-acl)# exit
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match ip address Strict-Control
Switch(config-route-map)# set ip next-hop 120.1.2.2
Switch(config-route-map)# exit
Switch(config)# interface vlan 100
Switch(config-if)# ip policy route-map myPolicy
Switch(config-if)#
```

72-9 set ip next-hop

Данная команда используется для настройки на маршрутизаторе следующего узла (Next Hop) для маршрутизации пакетов, которые соответствуют настроенным правилам последовательностей карты маршрутов. Используйте форму **no**, чтобы удалить определенные следующие узлы.

```
set ip next-hop {IP-ADDRESS [...IP-ADDRESS] | recursive IP-ADDRESS}
no set ip next-hop {IP-ADDRESS [...IP-ADDRESS] | recursive IP-ADDRESS}
```

Параметры

<i>IP-ADDRESS</i>	Укажите IP-адрес Next Hop для маршрутизации пакетов.
recursive	Укажите IP-адрес рекурсивного Next Hop маршрутизатора.

По умолчанию

Нет

Режим ввода команды

Route-map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

На маршрутизаторе возможна настройка нескольких Next Hop. Если Next Hop уже были настроены, новые настроенные Next Hop будут добавлены в список ранее настроенных узлов. Если первый указанный Next Hop на маршрутизаторе отключен, для маршрутизации пакетов будет выбран второй указанный Next Hop.

Пример

В данном примере показан процесс настройки политики PBR, с помощью которой пакеты будут отправлены на Next Hop 120.1.2.2. IP-адрес источника – 10.1.1.0/24. Принимающий интерфейс – VLAN 100. Сначала создается основной список доступа IP, разрешающий префикс 10.1.1.0/24. Созданный список – Strict-Control. Затем создается карта маршрутов, соответствующая IP-адресу из списка префиксов созданного списка «Strict-Control». Созданная карта маршрутов – myPolicy. Для использования карты маршрутов «myPolicy» необходимо задать IP-адрес политики PBR в режиме VLAN Interface Configuration Mode.

```
Switch# configure terminal
Switch(config)# ip access-list Strict-Control
Switch(config-ip-acl)# permit 10.1.1.0 0.0.0.255 any
Switch(config-ip-acl)# exit
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match ip address Strict-Control
Switch(config-route-map)# set ip next-hop 120.1.2.2
Switch(config-route-map)# exit
Switch(config)# interface vlan 100
Switch(config-if)# ip policy route-map myPolicy
Switch(config-if)#
```

72-10 set ip precedence

Данная команда используется для настройки значения приоритета (Precedence) для заголовка IP. Используйте форму **no**, чтобы удалить настройки.

```
set ip precedence {NUMBER | NAME}
no set ip precedence
```

Параметры

<i>NUMBER</i>	Укажите число для значения приоритета для заголовка IP.
---------------	---

Ниже представлены числа и соответствующие имена для них:

- 0 – Routine
- 1 – Priority
- 2 – Immediate
- 3 – Flash
- 4 – Flash-override
- 5 – Critical
- 6 – Internet
- 7 – Network

NAME

Укажите имя значения приоритета для заголовка IP.

По умолчанию

Нет

Режим ввода команды

Route-map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить значение приоритета для заголовка IP. Команда доступна, только если политика маршрутизации включает в себя пакеты IPv4. Приоритет можно установить при помощи номера или соответствующего имени.

Пример

В данном примере показано, как настроить значение приоритета IP для пакетов, соответствующих карте маршрутов. Настроенное значение – 5 (критическое).

```
Switch# configure terminal
Switch(config)# route-map example permit 10
Switch(config-route-map)# match ip address IPACL_01
Switch(config-route-map)# set ip precedence 5
Switch(config-route-map)#
```

72-11 set metric

Данная команда используется для изменения метрики маршрутов. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
set metric VALUE
no set metric
```

Параметры

VALUE

Укажите метрику маршрута в диапазоне от 0 до

4294967294.

По умолчанию

Нет

Режим ввода команды

Route-map Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы изменить метрику маршрутов.

Пример

В данном примере показано, как настроить метрику маршрутов, которые соответствуют карте маршрутов. Настроенная метрика – 100.

```
Switch# configure terminal
Switch(config)# route-map example permit 10
Switch(config-route-map)# match ip address IPACL_01
Switch(config-route-map)# set metric 100
Switch(config-route-map)#
```

73. Команды Router Advertisement (RA) Guard

73-1 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы создать политику RA Guard Policy и войти в режим RA Guard Policy Configuration Mode.

Пример

В данном примере показано, как создать политику RA Guard Policy под именем «policy1».

```
Switch# configure terminal
Switch(config)# ipv6 nd rguard policy policy1
Switch(config-ra-guard)#
```

73-2 device-role

Данная команда используется для указания роли подключенного устройства. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
device-role {host | router}
no device-role
```

Параметры

host	Укажите, чтобы настроить подключенное устройство в качестве узла (Host).
-------------	--

router	Укажите, чтобы настроить подключенное устройство в качестве маршрутизатора (Router).
---------------	--

По умолчанию

Роль по умолчанию – Host.

Режим ввода команды

RA Guard Policy Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать роль подключенного устройства. Так как по умолчанию устройство выполняет роль узла, получаемые Router Advertisement (RA) и сообщения переадресации будут заблокированы. Если устройство настроено в качестве маршрутизатора, Router Solicitation (RS), Router Advertisement (RA) и сообщения переадресации будут разрешены на данном порту.

Пример

В данном примере показано, как создать политику RA Guard Policy под именем «raguard1» и настроить устройство в качестве узла.

```
Switch# configure terminal
Switch(config)# ipv6 nd raguard policy raguard1
Switch(config-ra-guard)# device-role host
Switch(config-ra-guard)#
```

73-3 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для устройства в роли маршрутизатора (Router), чтобы отфильтровать RA-сообщения на основе IP-адреса отправителя. Если команда **match ipv6 access-list** не настроена, все RA-сообщения будут игнорироваться. Список доступа настраивается с помощью команды **ipv6 access-list**.

Пример

В данном примере показано, как создать политику RA Guard Policy и настроить проверку соответствия IPv6-адресов списку доступа «list1».

```
Switch# configure terminal
Switch(config)# ipv6 nd rguard policy rguard1
Switch(config-ra-guard)# match ipv6 access-list list1
Switch(config-ra-guard)#
```

73-4 ipv6 nd rguard attach-policy

Данная команда используется для применения политики RA Guard Policy на определенном интерфейсе. Используйте форму **no**, чтобы удалить привязку.

```
ipv6 nd rguard attach-policy [POLICY-NAME]
no ipv6 nd rguard
```

Параметры

<i>POLICY-NAME</i>	(Опционально) Укажите имя политики RA Guard Policy.
--------------------	---

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Может быть применена только одна политика RA Policy. Если имя политики не указано, политика по умолчанию настроит устройство в качестве узла.

Пример

В данном примере показано, как применить политику RA Guard Policy на интерфейсе Ethernet 1/0/3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ipv6 nd rguard attach-policy rguard1
Switch(config-if)#
```

73-5 show ipv6 nd rguard policy

Данная команда используется для отображения информации о политике RA Guard Policy.

show ipv6 nd rguard policy [*POLICY-NAME*]

Параметры

<i>POLICY-NAME</i>	(Опционально) Укажите имя политики RA Guard Policy.
--------------------	---

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Если имя политики указано, отображаться будет информация только для указанной политики. Если имя политики не указано, отображаться будет информация для всех политик.

Пример

В данном примере показано, как отобразить конфигурацию политики под именем «rguard1» на всех интерфейсах, на которых применена данная политика.

```
Switch(config)#show ipv6 nd rguard policy rguard1

Policy rguard1 configuration:
  Device Role: host
  Source Address Match Access List: list1
  Target: eth1/0/3

Switch(config)#
```

74. Команды Routing Information Protocol (RIP)

74-1 address-family (RIP)

Данная команда используется для входа в режим Router Address Family Configuration (RIP) Mode и для настройки определенного семейства адресов (Address Family). Используйте форму **no**, чтобы удалить определенное семейство адресов.

```
address-family ipv4
no address-family ipv4
```

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Router Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы войти в режим Router Address Family Configuration (RIP) Mode и настроить определенное семейство адресов.

Пример

В данном примере показано, как войти в режим Router Address Family Configuration (RIP) Mode.

```
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#address-family ipv4
Switch(config-router-af)#
```

74-2 default-metric (RIP)

Данная команда используется для указания значения метрики (Metric) по умолчанию для маршрутов, перераспределяемых RIP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
default-metric METRIC-VALUE
no default-metric
```

Параметры

<i>METRIC-VALUE</i>	Укажите значение метрики по умолчанию в диапазоне от 0 до 16.
---------------------	---

По умолчанию

Значение по умолчанию – 0.

Режим ввода команды

Router Configuration Mode
Router Address Family Configuration (RIP) Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать значение метрики по умолчанию для маршрутов, перераспределяемых из других протоколов маршрутизации. Перераспределяемые маршруты, информация о которых была получена от других протоколов, имеют несовместимое значение метрики для RIP. Для синхронизации метрики необходимо указать ее значение повторно.

Пример

В данном примере показано, как настроить значение метрики по умолчанию для маршрутов, перераспределяемых OSPF. Настроенное значение – 5.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# default-metric 5
Switch(config-router)# redistribute ospf
Switch(config-router)#
```

74-3 distance (RIP)

Данная команда используется для указания административного расстояния (Administrative Distance) маршрутов, информация о которых была получена от протоколов маршрутизации IPv4. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

distance *DISTANCE*
no distance

Параметры

<i>DISTANCE</i>	Укажите административное расстояние в диапазоне от 1 до 255. Чем ниже значение, тем выше приоритет маршрута.
-----------------	--

По умолчанию

Расстояние RIP по умолчанию – 100.

Режим ввода команды

Router Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить расстояние, которое представляет рейтинг доверия маршрута. В качестве расстояния может быть указано целое число от 1 до 255. Маршрут, значение расстояния которого ниже, имеет более высокий приоритет, чем маршрут со значением выше. Маршруты, расстояние которых равно 255, не будут установлены для маршрутизации пакетов, поскольку в данном случае маршруты не являются доверенными.

Пример

В данном примере показано, как настроить расстояние маршрутов RIP. Настроенное значение – 100.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# distance 100
Switch(config-router)#
```

74-4 ip rip authentication mode

Данная команда используется для указания типа аутентификации, который используется для пакетов RIP Version 2. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip rip authentication mode text
no ip rip authentication mode
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применима только для RIP Version 2. RIP Version 1 не поддерживает аутентификацию.

Пример

В данном примере показано, как включить аутентификацию на интерфейсе VLAN 2.

```
Switch# configure terminal
Switch(config)# interface vlan 2
Switch(config-if)# ip rip authentication mode text
Switch(config-if)#
```

74-5 ip rip authentication text-password

Данная команда используется для включения аутентификации для пакетов RIP Version 2 и для указания ключа, который будет использоваться на интерфейсе. Используйте форму **no**, чтобы отменить аутентификацию.

```
ip rip authentication text-password PASSWORD
no ip rip authentication text-password
```

Параметры

<i>PASSWORD</i>	Укажите пароль.
-----------------	-----------------

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения аутентификации для пакетов RIP Version 2 и для указания ключа, который будет использоваться на интерфейсе.

Пример

В данном примере показано, как настроить аутентификацию на интерфейсе VLAN 3.

```
Switch# configure terminal
Switch(config)# interface vlan 3
Switch(config-if)# ip rip authentication mode text
Switch(config-if)# ip rip authentication text-password test1
Switch(config-if)#
```

74-6 ip rip receive version

Данная команда используется для указания RIP Version для пакетов, которые будут получены на интерфейсе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip rip receive version [1] [2]
no ip rip receive version
```

Параметры

1	(Опционально) Укажите, чтобы получать пакеты RIP Version 1.
2	(Опционально) Укажите, чтобы получать пакеты RIP Version 2.

По умолчанию

По умолчанию используются глобальные настройки.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать RIP Version для пакетов, которые будут получены на интерфейсе. Если версия не указана, применяются глобальные настройки.

Пример

В данном примере показано, как настроить получение пакетов RIP Version 1 и RIP Version 2 на интерфейсе VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip rip receive version 1 2
Switch(config-if)#
```

74-7 ip rip send version

Данная команда используется для указания RIP Version для пакетов, которые будут отправлены с интерфейса. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip rip send version [1 2]
no ip rip send version
```

Параметры

1	(Опционально) Укажите, чтобы отправлять пакеты RIP Version 1.
2	(Опционально) Укажите, чтобы отправлять пакеты RIP Version 2.

По умолчанию

По умолчанию используются глобальные настройки.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать RIP Version для пакетов, которые будут отправлены с интерфейса. Если версия не указана, применяются глобальные настройки.

Пример

В данном примере показано, как включить отправку пакетов RIP Version 1 на интерфейсе VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan 100
Switch(config-if)# ip rip send version 1
Switch(config-if)#
```

74-8 ip rip v2-broadcast

Данная команда используется для включения отправки пакетов обновлений RIP Version 2 в качестве широковещательных пакетов (broadcast), а не многоадресных пакетов (multicast). Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip rip v2-broadcast
no ip rip v2-broadcast
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

RIP Version 2, в отличие от Version 1, позволяет отправлять широковещательные пакеты вместо многоадресных пакетов в целях снижения нагрузки на ненужных узлах в локальной сети для обработки широковещательного пакета.

Используйте данную команду, чтобы настроить широковещательную рассылку обновлений RIP Version 2 на устройства, которые не прослушивают многоадресные пакеты. При включенной функции пакеты Version 2 будут отправлены на широковещательный IP-адрес вместо IP-адреса multicast 224.0.0.9.

Пример

В данном примере показано, как настроить отправку широковещательных пакетов RIP Version 2 на интерфейсе VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan 100
Switch(config-if)# ip rip send version 2
Switch(config-if)# ip rip v2-broadcast
Switch(config-if)#
```

74-9 network

Данная команда используется для указания сети, в которой будет использоваться RIP. Используйте форму **no**, чтобы удалить запись.

```
network NETWORK-PREFIX
no network NETWORK-PREFIX
```

Параметры

<i>NETWORK-PREFIX</i>	Укажите префикс подсети.
-----------------------	--------------------------

По умолчанию

Нет

Режим ввода команды

Router Configuration Mode
Router Address Family Configuration (RIP) Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать сети, в которых будут отправлены и получены обновления маршрутизации. RIP будет активирован на интерфейсе, для которого задана подсеть, принадлежащая указанной в команде сети.

Пример

В данном примере показано, как указать RIP в качестве протокола маршрутизации, который будет использоваться на всех интерфейсах, подключенных к сетям 192.168.70.0/24 и к сети 10.99.0.0/16.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# network 192.168.70.0
Switch(config-router)# network 10.99.0.0
Switch(config-router)#
```

74-10 passive-interface

Данная команда используется для отключения отправки обновлений маршрутизации на интерфейсе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
passive-interface {default | INTERFACE-ID}
no passive-interface {default | INTERFACE-ID}
```

Параметры

default	Укажите, чтобы включить пассивный режим по умолчанию глобально на всех интерфейсах.
<i>INTERFACE-ID</i>	Укажите ID интерфейса, на котором необходимо включить пассивный режим. Если ID интерфейса не указан, будет глобально включен пассивный режим по умолчанию.

По умолчанию

Обновления маршрутизации по умолчанию отправляются.

Режим ввода команды

Router Configuration Mode
Router Address Family Configuration (RIP) Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

При использовании данной команды маршрутизатор не будет отправлять многоадресные пакеты RIP через интерфейс. Однако обработка пакетов RIP, полученных на данном интерфейсе от других маршрутизаторов, не будет приостановлена.

Пример

В данном примере показано, как отключить отправки обновлений маршрутизации на интерфейсе VLAN 1.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# passive-interface vlan 1
Switch(config-router)#
```

74-11 redistribute (RIP)

Данная команда используется для перераспределения маршрутов из других доменов маршрутизации в RIP. Используйте форму **no**, чтобы отменить перераспределение маршрута из определенного протокола.

redistribute *PROTOCOL* [**metric** *METRIC-VALUE*] [**route-map** *MAP-NAME*]
no redistribute *PROTOCOL* [**metric** *METRIC-VALUE*] [**route-map** *MAP-NAME*]

Параметры

<i>PROTOCOL</i>	Укажите протокол, маршруты которого необходимо перераспределить. Доступны следующие ключевые слова: connected , ospf , static . Укажите static для перераспределения статических IP-маршрутов. Укажите connected для перераспределения маршрутов, установленных автоматически на основе настроек IP-адреса на интерфейсе.
metric <i>METRIC-VALUE</i>	(Опционально) Укажите значение метрики для перераспределяемых маршрутов. Доступный диапазон значений: от 0 до 16.
route-map <i>MAP-NAME</i>	(Опционально) Укажите карту маршрута (Route Map) для фильтрации маршрутов, перераспределяемых в текущий протокол маршрутизации. Если не указано, будут перераспределены все маршруты.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Router Configuration Mode
 Router Address Family Configuration (RIP) Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если метрика не указана или в качестве ее значения установлен 0, будут применимы следующие правила:

- Метрика перераспределяемого статического или подключенного маршрута будет равна одному, если метрика не указана или в качестве ее значения установлен 0.
- Метрика перераспределяемого в RIP маршрута, информация о котором была получена от других протоколов, будет определена командой **default-metric**, если метрика не указана.
- Метрика перераспределяемого в RIP маршрута, информация о котором была получена от других протоколов, будет равна одному, если в качестве ее значения установлен 0.

Если метрика по умолчанию не указана, то автоматически будет назначена исходная метрика из перераспределяемого протокола.

Если настроенной карты маршрута не существует, ни один из маршрутов не будет разрешен. Если для настроенной последовательности карты маршрута не определена запись соответствия, то все маршруты будут соответствовать этой последовательности.

Пример

В данном примере показано, как настроить маршруты OSPF для перераспределения в домен RIP. Метрика, настроенная в OSPF, будет переназначена. Переназначенное значение – 10.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# redistribute ospf metric 10
Switch(config-router)#
```

74-12 router rip

Данная команда используется для настройки маршрутизации RIP. Используйте форму **no**, чтобы отключить маршрутизацию RIP.

```
router rip
no router rip
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы войти в режим Router Configuration Mode протокола RIP и включить функцию RIP. Используйте форму **no**, чтобы удалить настройки в режиме RIP Router Mode и отключить функцию RIP.

Пример

В данном примере показано, как настроить маршрутизацию RIP.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)#
```

74-13 show ip rip database

Данная команда используется для отображения базы данных маршрутизации Routing Information Protocol (RIP).

```
show ip rip database [IP-ADDRESS MASK | NETWORK-PREFIX/PREFIX-LENGTH]
```

Параметры

<i>IP-ADDRESS MASK</i>	(Опционально) Укажите адрес, информацию о маршрутизации которого необходимо отобразить.
<i>NETWORK-PREFIX/PREFIX-LENGTH</i>	(Опционально) Укажите префикс подсети и длину префикса сети, которую необходимо отобразить.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы отобразить запись базы данных маршрутизации RIP.

Пример

В данном примере показано, как отобразить базу данных маршрутизации RIP.

```
Switch#show ip rip database

Codes: R - RIP, Rc - RIP connected, K - Kernel,
       C - Connected, S - Static, O - OSPF, B - BGP, I-IS-IS, A - Aggregate

   Network          Next Hop        Metric From                If          Time
Rc  11.0.0.0/8
R   105.100.0.0/24   11.0.0.5        2     11.0.0.5             vlan 11    00T0H0M2S
Rc  107.100.0.0/16
R   212.254.254.0/24 11.0.0.254      2     11.0.0.254           vlan 11    00T0H0M10S

Total Entries: 4 entries, 4 routes

Switch#
```

74-14 show ip rip interface

Данная команда используется для отображения определенной информации о RIP на интерфейсе.

```
show ip rip interface
```

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для отображения определенной информации о RIP на интерфейсе.

Пример

В данном примере показано, как отобразить определенную информацию о RIP на интерфейсе.

```
Switch#show ip rip interface

vlan 11 is up, line protocol is up:
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Send v2-broadcast: Disable
    Authentication Mode: none
    Passive interface: Disable
    BFD Status: Disable
    IP interface address:
      11.0.0.3/8:

vlan 1 is up, line protocol is up:
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Send v2-broadcast: Disable
    Authentication Mode: none
    Passive interface: Disable
    BFD Status: Disable
    IP interface address:
      107.100.0.1/16:

Total Entries : 2

Switch#
```

74-15 timers basic

Данная команда используется для настройки таймеров сетевого протокола RIP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
timers basic UPDATE INVALID FLUSH
no timers
```

Параметры

<i>UPDATE</i>	Укажите интервал Update, по истечению которого будет отправлено сообщение с обновлениями. Доступный диапазон значений: от 5 до 65535 секунд.
<i>INVALID</i>	Укажите таймер Invalidate. Доступный диапазон значений: от 1 до 65535 секунд.
<i>FLUSH</i>	Укажите таймер Flush. Доступный диапазон значений: от 1 до 65535 секунд.

По умолчанию

По умолчанию значение таймера Update – 30 секунд.

По умолчанию значение таймера Invalidate – 180 секунд.

По умолчанию значение таймера Flush – 120 секунд.

Режим ввода команды

Router Configuration Mode

Router Address Family Configuration (RIP) Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы изменить таймеры протокола RIP.

Пример

В данном примере показано, как настроить таймеры RIP. Настроенные таймеры: Update – 10, Invalid – 80 и Flush – 160.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# timers basic 10 80 160
Switch(config-router)#
```

74-16 version

Данная команда используется для глобальной настройки RIP Version по умолчанию для всех интерфейсов. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

version {1 | 2}
no version

Параметры

1	(Опционально) Укажите, чтобы получать и отправлять пакеты RIP Version 1.
2	(Опционально) Укажите, чтобы получать и отправлять пакеты RIP Version 2.

По умолчанию

По умолчанию могут быть отправлены только пакеты RIP Version 1, а получены пакеты RIP Version 1 и RIP Version 2.

Режим ввода команды

Router Configuration Mode
Router Address Family Configuration (RIP) Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить RIP Version по умолчанию. RIP Version, заданная командами **ip rip send version** и **ip rip receive version** для интерфейса, будет перезаписана.

Пример

В данном примере показано, как указать RIP Version 2 в качестве RIP Version.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# version 2
Switch(config-router)#
```

75. Команды Routing Information Protocol Next Generation (RIPng)

75-1 clear ipv6 rip

Данная команда используется для удаления базы данных маршрутов RIPng.

clear ipv6 rip

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

После удаления базы данных маршрутов RIPng база данных маршрутизации будет очищена и заново заполнена.

Пример

В данном примере показано, как удалить базу данных RIPng.

```
Switch# clear ipv6 rip
Clear ipv6 rip? (y/n) [n] y
Switch#
```

75-2 default-metric (RIPng)

Данная команда используется для указания значения метрики (Metric) по умолчанию для маршрутов, перераспределяемых RIPng. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

default-metric *METRIC-VALUE*

no default-metric

Параметры

METRIC-VALUE

Укажите значение метрики по умолчанию в диапазоне от 0

до 16.

По умолчанию

Значение по умолчанию – 0.

Режим ввода команды

Router Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать значение метрики по умолчанию для маршрутов, перераспределяемых из других протоколов маршрутизации. Перераспределяемые маршруты, информация о которых была получена от других протоколов, имеют несовместимое значение метрики для IPv6 RIP. Для синхронизации метрики необходимо указать ее значение повторно.

Пример

В данном примере показано, как настроить значение метрики по умолчанию для маршрутов, перераспределяемых RIPng. Настроенное значение – 5.

```
Switch# configure terminal
Switch(config)# ipv6 router rip
Switch(config-rtr)# default-metric 5
Switch(config-rtr)# redistribute ospf
Switch(config-rtr)#
```

75-3 distance (RIPng)

Данная команда используется для указания административного расстояния (Administrative Distance) маршрутов, информация о которых была получена от протоколов маршрутизации IPv6. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

distance *DISTANCE*
no distance

Параметры

<i>DISTANCE</i>	Укажите административное расстояние в диапазоне от 1 до 254. Чем ниже значение, тем выше приоритет маршрута.
-----------------	--

По умолчанию

Расстояние RIPng по умолчанию – 120.

Режим ввода команды

Router Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить расстояние, которое представляет рейтинг доверия маршрута. В качестве расстояния может быть указано целое число от 1 до 254. Маршрут, значение расстояния которого ниже, имеет более высокий приоритет, чем маршрут со значением выше.

Пример

В данном примере показано, как настроить расстояние маршрутов RIPv6. Настроенное значение – 100.

```
Switch# configure terminal
Switch(config)# ipv6 router rip
Switch(config-rtr)# distance 100
Switch(config-rtr)#
```

75-4 ipv6 rip enable

Данная команда используется для включения маршрутизации RIP для IPv6 на интерфейсе. Используйте форму **no**, чтобы отключить маршрутизацию RIP для IPv6 на интерфейсе.

```
ipv6 rip enable
no ipv6 rip enable
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить IPv6 RIP на необходимых интерфейсах.

Пример

В данном примере показано, как включить маршрутизацию RIP для IPv6 на VLAN 1.


```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 rip enable
Switch(config-if)#
```

75-5 ipv6 rip metric-offset

Данная команда используется для указания значения, которое необходимо добавить к метрике маршрута IPv6 RIP, полученного на настраиваемом интерфейсе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ipv6 rip metric-offset METRIC-VALUE
no ipv6 rip metric-offset
```

Параметры

<i>METRIC-VALUE</i>	Укажите значение, которое необходимо добавить к метрике маршрута IPv6 RIP, полученного на настраиваемом интерфейсе. Доступный диапазон значений: от 1 до 16.
---------------------	--

По умолчанию

Значение по умолчанию – 1.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Метрика относится к счетчику промежуточных узлов. Перед вставкой полученного маршрута IPv6 RIP в таблицу маршрутизации, к метрике данного маршрута будет добавлено значение по умолчанию – 1. Используйте данную команду, чтобы настроить метрику маршрутов, полученных на разных интерфейсах. Данная настройка влияет на приоритет маршрута.

Пример

В данном примере показано, как настроить метрику с шагом 3 для маршрутов, полученных на VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 rip metric-offset 3
Switch(config-if)#
```

75-6 ipv6 router rip

Данная команда используется для настройки маршрутизации RIP для IPv6. Используйте форму **no**, чтобы отключить маршрутизацию RIP для IPv6.

```
ipv6 router rip  
no ipv6 router rip
```

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы войти в режим Router Configuration Mode и настроить маршрутизацию RIP для IPv6. Используйте форму **no**, чтобы отключить маршрутизацию RIP для IPv6.

Пример

В данном примере показано, как настроить маршрутизацию RIP для IPv6.

```
Switch# configure terminal  
Switch(config)# ipv6 router rip  
Switch(config-rtr)#
```

75-7 poison-reverse

Данная команда используется для включения технологии обратного исправления (Poison Reverse) для IPv6 RIP. Используйте форму **no**, чтобы отключить Poison Reverse.

```
poison-reverse  
no poison-reverse
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Router Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить технологию обратного исправления (Poison Reverse) в обновлениях маршрутизации RIP. При включении Poison Reverse маршруты, информация о которых была получена с интерфейса, будут анонсированы в тот же интерфейс с недоступной метрикой.

Пример

В данном примере показано, как включить Poison Reverse для IPv6 RIP.

```
Switch# configure terminal
Switch(config)# ipv6 router rip
Switch(config-rtr)# poison-reverse
Switch(config-rtr)#
```

75-8 redistribute (RIPng)

Данная команда используется для перераспределения маршрутов из других доменов маршрутизации в RIP. Используйте форму **no**, чтобы отменить перераспределение маршрута с определенных протоколов.

```
redistribute PROTOCOL [metric METRIC-VALUE]
no redistribute PROTOCOL
```

Параметры

<i>PROTOCOL</i>	Укажите протокол, маршруты которого необходимо перераспределить. Доступны следующие ключевые слова: connected , ospf , static . Укажите static для перераспределения статических IP-маршрутов. Укажите connected для перераспределения маршрутов, установленных автоматически на основе настроек IP-адреса на интерфейсе.
metric <i>METRIC-VALUE</i>	(Опционально) Укажите метрику для перераспределяемых маршрутов. Доступный диапазон значений: от 0 до 16.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Router Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если метрика не указана или в качестве ее значения установлен 0, будут применимы следующие правила:

- Метрика перераспределяемого статического или подключенного маршрута будет равна одному, если метрика не указана или в качестве ее значения установлен 0.
- Метрика перераспределяемого в RIP маршрута, информация о котором была получена от других протоколов, будет определена командой **default-metric**, если метрика не указана.
- Метрика перераспределяемого в RIP маршрута, информация о котором была получена от других протоколов, будет равна одному, если в качестве ее значения установлен 0.

Если метрика по умолчанию не указана, то автоматически будет назначена исходная метрика из перераспределяемого протокола.

Пример

В данном примере показано, как настроить маршруты OSPF для перераспределения в домен RIP. Значение метрики, настроенной в OSPF, будет переназначено. Переназначенное значение – 10.

```
Switch# configure terminal
Switch(config)# ipv6 router rip
Switch(config-rtr)# redistribute ospf metric 10
Switch(config-rtr)#
```

75-9 passive-interface

Данная команда используется для отключения отправки обновлений маршрутизации на интерфейсе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

passive-interface {default | INTERFACE-ID}
no passive-interface {default | INTERFACE-ID}

Параметры

default	Укажите, чтобы включить пассивный режим по умолчанию глобально на всех интерфейсах.
INTERFACE-ID	Укажите ID интерфейса, на котором необходимо включить пассивный режим.

По умолчанию

Обновления маршрутизации по умолчанию отправляются.

Режим ввода команды

Router Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

При использовании данной команды маршрутизатор не будет отправлять пакеты RIPng через интерфейс. Однако обработка пакетов RIPng, полученных на данном интерфейсе от других маршрутизаторов, не будет приостановлена.

Пример

В данном примере показано, как отключить отправку обновлений маршрутизации на интерфейсе.

```
Switch#configure terminal
Switch(config)#ipv6 router rip
Switch(config-rtr)#passive-interface vlan 1
Switch(config-rtr)#
```

75- 10 show ipv6 rip

Данная команда используется для отображения информации о RIPng на интерфейсе.

show ipv6 rip [database]

Параметры

database	(Опционально) Укажите для отображения записи базы данных маршрутизации RIP.
-----------------	---

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию о настройках протокола RIP.

Используйте команду **show ipv6 rip database**, чтобы отобразить запись базы данных маршрутизации RIP.

Пример

В данном примере показано, как отобразить информацию о настройках RIP.

```
Switch#show ipv6 rip

IPv6 RIP process, port 521, multicast-group FF02::9
Administrative distance is 71
Maximum paths is 16
Updates every 30 seconds, expire after 180 seconds
Garbage collect after 120 seconds
Split horizon is on; poison reverse is on
Periodic updates 6, trigger updates 1

Interfaces:
  vlan 1
  vlan 11      (passive)
Redistribution:
  Redistributing static with metric 10

Switch#
```

75-11 split-horizon

Данная команда используется для включения технологии Split Horizon для IPv6 RIP. Используйте форму **no**, чтобы отключить Split Horizon.

split-horizon
no split-horizon

Параметры

Нет

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Router Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить технологию Split Horizon в обновлениях маршрутизации IPv6 RIP. При включении Split Horizon маршруты, информация о которых была получена с интерфейса, не будут анонсированы в тот же интерфейс.

Пример

В данном примере показано, как отключить Split Horizon для IPv6 RIP.

```
Switch# configure terminal
Switch(config)# ipv6 router rip
Switch(config-rtr)# no split-horizon
Switch(config-rtr)#
```

75-12 timers

Данная команда используется для настройки таймеров сетевого протокола IPv6 RIP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
timers UPDATE INVALID FLUSH
no timers
```

Параметры

<i>UPDATE</i>	Укажите интервал Update, по истечению которого будет отправлено сообщение с обновлениями. Доступный диапазон значений: от 5 до 65535 секунд.
<i>INVALID</i>	Укажите таймер Invalidate. Доступный диапазон значений: от 1 до 65535 секунд.
<i>FLUSH</i>	Укажите таймер Flush. Доступный диапазон значений: от 1 до 65535 секунд.

По умолчанию

По умолчанию таймер Update – 30 секунд.
 По умолчанию таймер Invalidate – 180 секунд.
 По умолчанию таймер Flush – 120 секунд.

Режим ввода команды

Router Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы изменить таймеры протокола IPv6 RIP.

Пример

В данном примере показано, как настроить таймеры RIP. Настроенные таймеры: Update – 10, Invalid – 40 и Flush – 160.

```
Switch# configure terminal
Switch(config)# ipv6 router rip
Switch(config-rtr)# timers 10 40 160
Switch(config-rtr)#
```

75-13 debug ipv6 rip

Данная команда используется для включения функции отладки IPv6 RIP. Используйте форму **no**, чтобы отключить функцию отладки IPv6 RIP.

```
debug ipv6 rip  
no debug ipv6 rip
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Перед использованием данной команды необходимо включить функцию отладки глобально.

Пример

В данном примере показано, как включить функцию отладки IPv6 RIP.

```
Switch# debug ipv6 rip  
Switch#
```

75-14 debug ipv6 rip interface

Данная команда используется для включения функции отладки IPv6 RIP на интерфейсе коммутатора. Используйте форму **no**, чтобы отключить функцию отладки IPv6 RIP на интерфейсе коммутатора.

```
debug ipv6 rip interface  
no debug ipv6 rip interface
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы включить/отключить функцию отладки IPv6 RIP на интерфейсе коммутатора. Если при включенной функции на интерфейсе изменится статус IPv6 RIP или произойдет какое-то другое событие, которое касается изменения статуса интерфейса, то отобразится информация об отладке.

Пример

В данном примере показано, как включить функцию отладки IPv6 RIP на интерфейсе коммутатора.

```
Switch# debug ipv6 rip interface
Switch#

The RIPng interface vlan 1 has changed the link state to UP
```

75-15 debug ipv6 rip packet-transmitting

Данная команда используется для включения отладки IPv6 RIP при передаче пакетов на коммутаторе. Используйте форму **no**, чтобы отключить отладку IPv6 RIP при передаче пакетов на коммутаторе.

```
debug ipv6 rip packet-transmitting
no debug ipv6 rip packet-transmitting
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы включить/отключить отладку IPv6 RIP при передаче пакетов на коммутаторе. Если при включенной функции будет отправлен хотя бы один пакет протокола IPv6 RIP, то отобразится информация об отладке.

Пример

В данном примере показано, как включить отладку IPv6 RIP при передаче пакетов на коммутаторе.

```
Switch# debug ipv6 rip packet-transmitting
Switch#

Send a RIPng response packet to FE80::1 , Index 1
```

75-16 debug ipv6 rip packet-receiving

Данная команда используется для включения отладки IPv6 RIP при получении пакетов на коммутаторе. Используйте форму **no**, чтобы отключить отладку IPv6 RIP при получении пакетов на коммутаторе.

```
debug ipv6 rip packet-receiving
no debug ipv6 rip packet-receiving
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы включить/отключить отладку IPv6 RIP при получении пакетов на коммутаторе. Если при включенной функции будет получен хотя бы один пакет протокола IPv6 RIP, то отобразится информация об отладке.

Пример

В данном примере показано, как включить отладку IPv6 RIP при получении пакетов на коммутаторе.

```
Switch# debug ipv6 rip packet-receiving
Switch#

Received a RIPng request packet from FE80::1
```

75-17 debug ipv6 rip route

Данная команда используется для включения отладки маршрутов IPv6 RIP на коммутаторе. Используйте форму **no**, чтобы отключить отладку маршрутов IPv6 RIP на коммутаторе.

```
debug ipv6 rip route
no debug ipv6 rip route
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы включить/отключить отладку маршрутов IPv6 RIP на коммутаторе. Если при включенной функции будет добавлен, обновлен или удален хотя бы один маршрут IPv6 RIP, то отобразится информация об отладке.

Пример

В данном примере показано, как включить отладку маршрута IPv6 RIP на коммутаторе.

```
Switch#debug ipv6 rip route
Switch#
Switch#
Add a RIPng route to V6 route table dst= 2016:3130:: nexthop= FE80::206:28FF:FED8:FEAC
Switch#
Switch#
```

76. Команды Safeguard Engine

76-1 clear cpu-protect counters

Данная команда используется для обнуления счетчиков защиты ЦПУ.

clear cpu-protect counters {all | sub-interface [manage | protocol | route] | type [PROTOCOL-NAME]}

Параметры

all	Укажите для обнуления всех счетчиков защиты ЦПУ.
sub-interface [manage protocol route]	Укажите для обнуления счетчиков защиты ЦПУ под-интерфейсов. Если под-интерфейс не указан, будут обнулены счетчики защиты ЦПУ всех под-интерфейсов.
type [PROTOCOL-NAME]	Укажите для обнуления счетчиков защиты ЦПУ определенного протокола. Если имя протокола не указано, будут обнулены счетчики защиты ЦПУ всех протоколов.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

При вводе команды без параметров будут обнулены все счетчики защиты ЦПУ.

Пример

В данном примере показано, как удалить всю статистику защиты ЦПУ.

```
Switch# clear cpu-protect counters all
Switch#
```

76-2 cpu-protect safeguard

Данная команда используется для включения или настройки функции Safeguard Engine. Используйте форму **no**, чтобы отключить функцию Safeguard Engine.

cpu-protect safeguard [threshold RISING-THRESHOLD FALLING-THRESHOLD]
no cpu-protect safeguard [threshold]

Параметры

threshold	(Опционально) Укажите, чтобы настроить пороговые значения загрузки, при которой будет включаться/отключаться функция Safeguard Engine.
<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 – 50.
Нижний порог загрузки ЦПУ по умолчанию – 20.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Safeguard Engine позволяет сохранить устройство в работоспособном состоянии при атаке, минимизируя рабочую загрузку коммутатора и одновременно давая возможность пересылать важные пакеты по сети в ограниченной полосе пропускания. Если загрузка ЦПУ превышает установленный верхний порог, коммутатор переходит в режим высокой загрузки (Exhausted Mode). В данном режиме коммутатор ограничивает полосу пропускания принимаемых ARP-пакетов и широковещательных IP- пакетов.

Пример

В данном примере показано, как включить Safeguard Engine и настроить пороговые значения. Верхнее пороговое значение – 60. Нижнее пороговое значение – 40.

```
Switch# configure terminal
Switch(config)# cpu-protect safeguard threshold 60 40
Switch(config)#
```

76-3 cpu-protect sub-interface

Данная команда используется для настройки пропускной способности (Rate Limit) трафика, предназначенного для ЦПУ по типам под-интерфейсов. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

cpu-protect sub-interface {manage | protocol | route} pps RATE
no cpu-protect sub-interface {manage | protocol | route}

Параметры

pps RATE	Укажите пороговое значение. Единица измерения – пакеты в секунду. Если установлено значение 0, будут отброшены все пакеты указанных типов под-интерфейса.
-----------------	---

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Причины, по которым пакеты предназначаются для ЦПУ, могут быть классифицированы по следующим трем группам: manage, protocol и route. Под-интерфейс – это логический интерфейс, предназначенный для разделения полученных пакетов ЦПУ на разные группы. Как правило, для корректной работы функций пакеты протокола должны иметь более высокий приоритет. Обычно ЦПУ не участвует в маршрутизации пакетов. В некоторых случаях, например, при изучении нового IP- адреса, или если не указан маршрут по умолчанию, некоторые пакеты будут 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)#
```

76-4 cpu-protect type

Данная команда используется для настройки пропускной способности (Rate Limit) трафика, предназначенного для ЦПУ типом протокола. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

cpu-protect type PROTOCOL-NAME pps RATE
no cpu-protect type PROTOCOL-NAME

Параметры

PROTOCOL-NAME	Укажите имя протокола, который необходимо настроить.
----------------------	--

pps RATE	Укажите пороговое значение. Единица измерения – пакеты в секунду. Если установлено значение 0, будут отброшены все пакеты указанного протокола.
-----------------	---

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

ЦПУ должно обрабатывать следующие пакеты: протоколы маршрутизации, протоколы 2 уровня и пакеты для управления. ЦПУ, перегруженное предназначенным для него трафиком, будет тратить много времени на обработку ненужного трафика, что повлияет на процессы маршрутизации. Чтобы уменьшить нагрузку на ЦПУ, используйте данную команду для настройки порогового значения пакетов указанного протокола.

В соответствии с назначением пакетов, предназначенных для ЦПУ, маршрутизатор создает три виртуальных под-интерфейса для обработки пакетов:

- **manage** – пакеты предназначены для любого интерфейса маршрутизатора или интерфейса системы управления сетью через протокол интерактивного доступа, такого как Telnet или SSH;
- **protocol** – управляющие пакеты протокола, которые могут быть идентифицированы маршрутизатором;
- **route** – другие пакеты, поступающие на маршрутизатор для маршрутизации, которые должны быть обработаны ЦПУ, прежде чем это будет сделано без участия ЦПУ.

В таблице ниже перечислены имена поддерживаемых протоколов для данной команды:

Имя протокола	Описание	Классификация (sub-интерфейс)
8021x	Port-based Network Access Control	Protocol
arp	IP Address Resolution Protocol (ARP)	Protocol
bgp	Border Gateway Protocol	Protocol
dhcp	Dynamic Host Configuration	Protocol
dns	Domain Name Services	Protocol
dvmrp	Distance Vector Multicast Routing Protocol	Protocol
gvrp	GARP VLAN Registration Protocol	Protocol
icmpv4	IPv4 Internet Control Message Protocol	Protocol
icmpv6-nighbor	IPv6 ICMP Neighbor Discover Protocol (NS/NA/RS/RA)	Protocol
icmpv6-other	IPv6 ICMP except NDP NS/NA/RS/RA	Protocol
igmp	Internet Group Management Protocol	Protocol
lasp	Link Aggregation Control Protocol	Protocol
ntp	Network Time Protocol	Protocol

ospf	Open Shortest Path First	Protocol
pim	Protocol Independent Multicast	Protocol
pppoe	Point-to-Point Protocol over Ethernet	Protocol
rip	Routing Information Protocol	Protocol
snmp	Simple Network Management Protocol	Manage
ssh	Secured shell	Manage
stp	Spanning Tree Protocol (802.1D)	Protocol
telnet	Telnet	Manage
tftp	Trivial File Transfer Protocol	Manage
vrrp	Virtual Router Redundancy Protocol	Protocol
web	HTTP and HTTPS	Manage

Пример

В данном примере показано, как настроить пороговое значение пакетов протокола OSPF. Настроенное пороговое значение – 1000 пакетов в секунду.

```
Switch# configure terminal
Switch(config)# cpu-protect type ospf pps 100
Switch(config)#
```

76-5 show cpu-protect safeguard

Данная команда используется для отображения настроек и статуса функции Safeguard Engine.

show cpu-protect safeguard

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить настройки и статус функции Safeguard Engine.

Пример

В данном примере показано, как отобразить настройки и текущий статус Safeguard Engine.


```
Switch#show cpu-protect safeguard

Safeguard Engine State: Disabled
Safeguard Engine Status: Normal
Utilization Thresholds:
  Rising   :50%
  Falling  :20%

Switch#
```

Отображаемые параметры

Safeguard Engine Status	Текущий режим загрузки ЦПУ. Возможны следующие строки для отображения: Exhausted: если загрузка ЦПУ превышает установленный верхний порог, коммутатор переходит в режим Exhausted Mode, и механизм Safeguard Engine начинает функционировать. Safeguard Engine не выключается до тех пор, пока загрузка не снизится до нижнего порога. Normal: Safeguard Engine не срабатывает.
--------------------------------	---

76-6 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

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить настроенные значения Rate Limit и Drop Count механизма Safeguard Engine указанной группы. Данные счетчики подсчитываются программно.

Пример

В данном примере показано, как отобразить настроенные значения Rate Limit и Drop Count механизма Safeguard Engine указанной группы.

```
Switch#show cpu-protect sub-interface manage

Sub-Interface: manage
Rate Limit: 10 pps

Unit  Total                               Drop
-----
1     103                                   12

Switch#
```

76-7 show cpu-protect type

Данная команда используется для отображения пропускной способности (Rate Limit) и статистики защиты ЦПУ.

show cpu-protect type {PROTOCOL-NAME}

Параметры

<i>PROTOCOL-NAME</i>	Укажите для отображения настроенного значения Rate Limit и статистики указанного протокола СМ-карты и всех существующих IO-карт.
----------------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить Rate Limit и статистику механизма Safeguard Engine.

Пример

В данном примере показано, как отобразить Rate Limit и статистику механизма Safeguard Engine.

```
Switch#show cpu-protect type dhcp
```

```
Type: dhcp
Rate Limit: 200 pps
```

Unit	Total	Drop
1	0	0

```
Switch#
```

76-8 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

Уровень команды по умолчанию

Уровень 12

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)#
```

77. Команды сервера Secure File Transfer Protocol (SFTP)

77-1 ip sftp server

Данная команда используется для включения SFTP-сервера. Используйте форму **no**, чтобы отключить SFTP-сервер.

```
ip sftp server
no ip sftp server
```

Параметры

Нет

По умолчанию

По умолчанию SFTP-сервер отключен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для глобального включения SFTP, протокола, используемого для безопасной передачи данных. Сам SFTP не обеспечивает аутентификацию и безопасность, поэтому работает как подсистема SSH-сервера. Для корректной работы SFTP необходимо включить SSH- сервер с помощью команды **ip ssh server**. При отключении SSH-сервера или SFTP-сервера все установленные сессии SFTP будут завершены.

При включенном SFTP-сервере управление файлами на коммутаторе возможно с помощью различных клиентов, таких как WinSCP, PSFTP, FileZilla и других.

Пример

В данном примере показано, как включить SFTP-сервер.

```
Switch# configure terminal
Switch(config)# ip ssh server
Switch(config)# ip sftp server
Switch(config)#
```

77-2 ip sftp timeout

Данная команда используется для настройки таймера пассивного состояния (Idle Timer) для SFTP- сервера на коммутаторе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ip sftp timeout SECONDS
```

no ip sftp timeout**Параметры**

<i>SECONDS</i>	Укажите значение таймера пассивного состояния (Idle Timer) для SFTP- сервера. Доступный диапазон значений: от 30 до 600 секунд. Сессия SFTP завершается, если по истечении времени таймера пассивного состояния, установленного для указанной сессии, SFTP-сервер не обнаруживает никаких операций.
----------------	---

По умолчанию

Таймер пассивного состояния (Idle Timer) для SFTP по умолчанию – 120 секунд.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать значение таймера пассивного состояния (Idle Timer) для SFTP-сервера. Новые настройки применимы только для сессий, установленных после ввода данной команды, текущие сессии не изменяются. Отмена сессии SFTP по истечении времени таймера пассивного состояния не влияет на соответствующие сессии SSH Shell. Соединение SSH будет прервано после завершения всех сессий SSH (сессии SFTP и сессии Shell).

Пример

В данном примере показано, как настроить значение таймера пассивного состояния (Idle Timer) для SFTP-сервера на 600 секунд.

```
Switch# configure terminal
Switch(config)# ip sftp timeout 600
Switch(config)#
```

77-3 show ip sftp

Данная команда используется для отображения настроек SFTP-сервера.

show ip sftp**Параметры**

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить настройки SFTP-сервера.

Пример

В данном примере показано, как отобразить глобальные настройки SFTP-сервера.

```
Switch# show ip sftp

IP SFTP server      : Enabled
Protocol version    : 3
Idle time out       : 120 secs

Switch#
```

78. Команды Secure Shell (SSH)

78-1 crypto key generate

Данная команда используется для генерирования пары ключей RSA или DSA.

crypto key generate {rsa [modulus *MODULUS-SIZE*] | dsa}

Параметры

rsa	Укажите для генерирования пары ключей RSA.
modulus <i>MODULUS-SIZE</i>	(Опционально) Укажите количество битов в модуле. Доступные значения для RSA: 360, 512, 768, 1024 и 2048. Если не указано, будет получено сообщение о необходимости указать значение.
dsa	Укажите для генерирования пары ключей DSA. Фиксированный размер ключа DSA – 1024 битов.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Данная команда используется для генерирования пары ключей RSA или DSA.

Пример

В данном примере показано, как создать ключ RSA.

```
Switch# crypto key generate rsa

The RSA key pairs already existed.
Do you really want to replace them? (y/n) [n]y
Choose the size of the key modulus in the range of 360 to 2048.The process may take
a few minutes.
Number of bits in the modulus [768]: 768
Generating RSA key...Done

Switch#
```

78-2 crypto key zeroize

Данная команда используется для удаления пары ключей RSA или DSA.

crypto key zeroize {rsa | dsa}

Параметры

rsa	Укажите, чтобы удалить пару ключей RSA.
dsa	Укажите, чтобы удалить пару ключей DSA.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы удалить пару открытых ключей SSH-сервера. Если обе пары ключей RSA и DSA удалены, SSH-сервер будет недоступен.

Пример

В данном примере показано, как удалить ключ RSA.

```
Switch# crypto key zeroize rsa
Do you really want to remove the key? (y/n)[n]: y
Switch#
```

78-3 ip ssh timeout

Данная команда используется для настройки параметров контроля SSH на коммутаторе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ip ssh {timeout SECONDS | authentication-retries NUMBER}
no ip ssh {timeout | authentication-retries}

Параметры

timeout SECONDS	Укажите временной интервал ожидания ответа от SSH-клиента для этапа согласования SSH. Доступный диапазон значений: от 30 до 600.
authentication-retries NUMBER	Укажите количество попыток аутентификации. Сессия завершается после всех неудачных попыток. Доступный диапазон значений: от 1 до 32.

По умолчанию

По умолчанию значение тайм-аута – 120 секунд.
По умолчанию количество попыток аутентификации – 3.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить параметры SSH-сервера на коммутаторе. С помощью параметра **authentication-retries** укажите максимальное количество попыток аутентификации перед завершением сессии.

Пример

В данном примере показано, как настроить значение тайм-аута SSH на 160 секунд.

```
Switch# configure terminal
Switch(config)# ip ssh timeout 160
Switch(config)#
```

В данном примере показано, как настроить значение попыток аутентификации. Настроенное значение – 2. Соединение будет прервано после 2 неудачных попыток.

```
Switch# configure terminal
Switch(config)# ip ssh authentication-retries 2
Switch(config)#
```

78-4 ip ssh server

Данная команда используется для включения SSH-сервера. Используйте форму **no**, чтобы отключить SSH-сервер.

ip ssh server
no ip ssh server

Параметры

Нет

По умолчанию

По умолчанию SSH-сервер отключен.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить SSH-сервер.

Пример

В данном примере показано, как включить SSH-сервер.

```
Switch# configure terminal
Switch(config)# ip ssh server
Switch(config)#
```

78-5 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить номер TCP-порта для SSH-сервера.

Пример

В данном примере показано, как изменить номер сервисного порта. Новый настроенный номер – 3000.

```
Switch# configure terminal
Switch(config)# ip ssh service-port 3000
Switch(config)#
```

78-6 show crypto key mypubkey

Данная команда используется для отображения пар открытых ключей RSA или DSA.

show crypto key mypubkey {rsa | dsa}

Параметры

rsa	Укажите, чтобы отобразить информацию об открытом ключе RSA.
dsa	Укажите, чтобы отобразить информацию об открытом ключе DSA.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы отобразить пары открытых ключей RSA или DSA.

Пример

В данном примере показано, как отобразить информацию об открытом ключе RSA.

```
Switch# show crypto key mypubkey rsa

% Key pair was generated at: 09:48:40, 2013-11-29
Key Size: 768 bits
Key Data:
AAAAB3Nz aC1yc2EA AAADAQAB AAAAQwCN 6IRFHCbf jsHvYjQG iCL0p2kz 2v38ULC8
kAKra/Ze mG7IW3eC 8STcrkr5 s7l9H/bh jG/oqkwj SlUJSGqR e/sj6Ws=

Switch#
```

78-7 show ip ssh

Данная команда используется для отображения пользовательских настроек конфигурации SSH.

show ip ssh

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить настройки конфигурации SSH.

Пример

В данном примере показано, как отобразить настройки конфигурации SSH.

```
Switch# show ip ssh

IP SSH server      : Enabled
IP SSH service port : 22
SSH server mode    : V2
Authentication timeout : 120 secs
Authentication retries : 3 times

Switch#
```

78-8 show ssh

Данная команда используется для отображения статуса подключений SSH-сервера.

show ssh

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить статус подключений SSH на коммутаторе.

Пример

В данном примере показано, как отобразить информацию о подключениях SSH.

```
Switch# show ssh

SID Ver. Cipher                               Userid                               Client IP Address
-----
0   V2  3des-cbc/sha1-96                             zhang3                               192.168.0.100
1   V2  3des-cbc/hmac-sha1                           lee4567890123456 2000::243

Total Entries: 2

Switch#
```

Отображаемые параметры

SID	Уникальный номер, идентифицирующий сессию SSH.
Ver	Версия SSH указанной сессии.
Cipher	Криптографический/Hashed Message Authentication Code (HMAC) алгоритм, используемый SSH-клиентом.
Userid	Имя пользователя сессии.
Client IP Address	IP-адрес клиента для установленной сессии SSH.

78-9 ssh user authentication-method

Данная команда используется для настройки методов аутентификации SSH для учетной записи пользователя. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
ssh user NAME authentication-method {password | publickey URL | hostbased URL host-name
HOSTNAME [IP-ADDRESS | IPV6-ADDRESS]}
no ssh user NAME authentication-method
```

Параметры

NAME	Укажите имя пользователя для настройки типа аутентификации. Имя пользователя должно быть существующей локальной учетной записью. Максимально допустимое количество символов – 32.
password	Укажите метод аутентификации по паролю для указанной учетной записи пользователя. Данный метод аутентификации используется по умолчанию.

publickey <i>URL</i>	Укажите метод аутентификации с открытым ключом для указанной учетной записи пользователя. Введите URL локального файла, который будет использоваться в качестве открытого ключа указанного пользователя.
hostbased <i>URL</i>	Укажите метод аутентификации на основе узла для указанной учетной записи пользователя. Введите URL локального файла, который будет использоваться в качестве ключа узла клиента.
host-name <i>HOSTNAME</i>	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

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы настроить метод аутентификации для пользователя. Имя пользователя должно быть пользователем, созданным при помощи команды **username**. По умолчанию используется метод аутентификации по паролю. Системой будет предложено ввести пароль.

Для аутентификации пользователя при помощи открытого ключа SSH скопируйте файл открытого ключа пользователя в файловую систему. Когда пользователь пытается войти в учетную запись на коммутаторе через SSH-клиента (используя метод открытого ключа SSH), SSH-клиент автоматически передаст коммутатору открытый ключ и подпись с закрытым ключом. Если и открытый ключ, и подпись верны, пользователь будет аутентифицирован, и вход в учетную запись коммутатора будет разрешен.

- Для аутентификации пользователя при помощи открытого ключа SSH или метода на основе узла необходимо указать файл открытого ключа пользователя или файл ключа узла клиента в одном и том же формате. Файл ключа может содержать несколько ключей. Каждый ключ должен быть определен одной строкой. Максимально допустимая длина строки составляет 8 Kb.
- Каждый ключ состоит из следующих разделенных пробелами полей: *keytype*, *base64-encoded key*, *comment*. Ввод полей *keytype* и *base64-encoded key* обязателен, ввод поля *comment* – 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)#
```

79. Команды Secure Sockets Layer (SSL)

79-1 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

Уровень команды по умолчанию

Уровень 15

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)#
```

79-2 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.
password <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.
tftp	Укажите URL источника для сетевого TFTP-сервера.
<i>IP-ADDRESS</i>	Укажите IP-адрес TFTP-сервера.
ca	Укажите, чтобы импортировать только сертификат ЦС.
local	Укажите, чтобы импортировать локальный сертификат и пары ключей.
both	Укажите, чтобы импортировать сертификат ЦС, локальный сертификат и пары ключей.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

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)#
```

79-3 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

<i>NAME</i>	Укажите для создания имени Trust Point.
-------------	---

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы настроить Trust Point, которая может выступать в качестве самоподтвержденного корневого центра сертификации или подчиненного ЦС. При использовании данной команды будет выполнен вход в режим CA-Trust-Point Configuration Mode.

Пример

В данном примере показано, как настроить Trust Point «TP1» и указать ее в качестве основной.

```
Switch# configure terminal
Switch(config)# crypto pki trustpoint TP1
Switch(ca-trustpoint)# primary
Switch(ca-trustpoint)#
```

79-4 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

Уровень команды по умолчанию

Уровень 15

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)#
```

79-5 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

Уровень команды по умолчанию

Уровень 15

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)#
```

79-6 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

Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 12

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  : webserver.crt
    local private key  : webserver.prv

Trustpoint Name      : TP2
  Imported certificates:
    CA                : chunagtel.ca
    local certificate  : openflow.crt
    local private key  : openflow.prv

Switch#
```

79-8 show ssl-service-policy

Данная команда используется для отображения политики SSL Service Policy.

show ssl-service-policy [POLICY-NAME]

Параметры

POLICY-NAME (Опционально) Укажите имя политики SSL Service Policy.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 12

Использование команды

Если имя политики SSL Service Policy не указано, отобразятся все SSL Service Policy.

Пример

В данном примере показано, как отобразить все SSL Service Policy.

```
Switch# show ssl-service-policy

SSL Policy Name      : policy1
Enabled 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
Session Cache Timeout: 600
Secure Trustpoint    : TP1

SSL Policy Name      : policy2
Enabled CipherSuites :
  RSA_WITH_3DES_EDE_CBC_SHA,
  RSA_WITH_RC4_128_MD5,
  RSA_EXPORT_WITH_RC4_40_MD5
Session Cache Timeout: 1200
Secure Trustpoint    : TP2

Switch#
```

79-9 ssl-service-policy

Данная команда используется для настройки политики SSL Service Policy.

```
ssl-service-policy POLICY-NAME [ciphersuite [dhe-dss-3des-ede-cbc-sha] [rsa-3des-ede-cbc-sha]
[rsa-rc4-128-sha] [rsa-rc4 128-md5] [rsa-export-rc4-40-md5] | secure-trustpoint TRUSTPOINT |session-
cache-timeout TIME-OUT]
```

```
no ssl-service-policy POLICY-NAME [ciphersuite [dhe-dss-3des-ede-cbc-sha] [rsa-3des-ede-cbc-
sha] [rsa-rc4-128-sha] [rsa-rc4-128-md5] [rsa-export-rc4-40-md5] | secure-trustpoint | session-cache-
timeout]
```

Параметры

POLICY-NAME

Укажите имя политики SSL Service Policy.

ciphersuite	<p>(Опционально) Укажите шифрование Cipher Suite, которое будет использоваться служба безопасности при установлении соединения с удаленным узлом.</p> <p>Используйте обмен ключами DH с шифрованием 3DES-EDE-CBC и SHA для дайджеста сообщений – dhe-dss-3des-ede-cbc-sha.</p> <p>Используйте обмен ключами RSA с шифрованием 3DES и DES-EDE3- CBC и Secure Hash Algorithm (SHA) для дайджеста сообщений – rsa-3des-ede-cbc-sha.</p> <p>Используйте обмен ключами RSA с 128-битным шифрованием RS4 и SHA для дайджеста сообщений – rsa-rc4-128-sha.</p> <p>Используйте обмен ключами RSA с 128-битным шифрованием RS4 и Message Digest 5 (MD5) для дайджеста сообщений – rsa-rc4-128-md5. Используйте обмен ключами RSA EXPORT с 40-битным шифрованием RS4 и MD5 для дайджеста сообщений – rsa-export-rc4-40-md5.</p> <p>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 no, чтобы отключить выбранные Cipher Suite.</p>
secure-trustpoint <i>TRUSTPOINT</i>	<p>(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 no, чтобы отменить указанные Trust Point и использовать встроенный сертификат/пары ключей.</p>
session-cache-timeout <i>TIME-OUT</i>	<p>(Опционально) Укажите значение тайм-аута в секундах для информации, хранящейся в кэше SSL-сессий. Доступный диапазон значений: от 60 до 86400. Если данный параметр не настроен, тайм-аут кэша сессий по умолчанию составляет 600 секунд. Используйте форму no, чтобы вернуть настройки по умолчанию для тайм-аута кэша SSL-сессий.</p>

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы настроить политику SSL Service Policy.

Пример

В данном примере показано, как настроить политику SSL Service Policy, которая ассоциирована с Trust Point «TP1». Настроенная политика SSL Service Policy – «ssl-server».

```
Switch# configure terminal
Switch(config)# ssl-service-policy ssl-server secure-trustpoint TP1
Switch(config)#
```


80. Команды sFlow

80-1 sflow receiver

Данная команда используется для настройки получателя для агента sFlow. Получатели не могут быть добавлены или удалены из агента sFlow. Используйте форму **no**, чтобы вернуть настройки по умолчанию для одного получателя.

```
sflow receiver INDEX [owner NAME] [expiry {SECONDS | infinite}] [max-datagram-size SIZE][host {IP-ADDRESS | IPV6-ADDRESS}] [udp-port PORT]
no sflow receiver INDEX
```

Параметры

<i>INDEX</i>	Укажите индекс получателя.
owner NAME	(Опционально) Укажите имя владельца получателя. Максимально допустимое количество символов – 32. При вводе данного параметра строка не должна оставаться пустой.
expiry SECONDS	(Опционально) Укажите время истечения записи. Параметр записи будет сброшен после истечения таймера. Доступный диапазон значений: от 0 до 2000000. При вводе данного параметра пользователь не может указать «0» в качестве значения таймера истечения.
infinite	(Опционально) Укажите отсутствие времени истечения записи.
max-datagram-size SIZE	(Опционально) Укажите максимальное количество байтов одной дейтаграммы sFlow. Доступный диапазон значений: от 700 до 1400.
host IP-ADDRESS	(Опционально) Укажите IPv4-адрес удаленного коллектора sFlow.
host IPV6-ADDRESS	(Опционально) Укажите IPv6-адрес удаленного коллектора sFlow.
udp-port PORT	(Опционально) Укажите UDP-порт удаленного коллектора sFlow. Значение по умолчанию – 6343. Доступный диапазон значений: от 1 до 65535.

По умолчанию

Строка с именем владельца по умолчанию пустая.
 Таймер истечения срока записи по умолчанию – 0 секунд.
 Максимальный размер дейтаграммы по умолчанию – 1400 байтов.
 IP-адрес получателя по умолчанию – 0.0.0.0.
 Номер UDP-порта по умолчанию – 6343.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Агент sFlow имеет фиксированное количество различаемых индексом получателей, созданных системой во время сброса. Эти получатели не могут быть удалены. Владелец записи должен быть настроен перед другими параметрами записи, и только когда запись находится в состоянии сброса (Reset). При вводе команды строка с именем владельца не должна оставаться пустой. Чтобы изменить настроенного владельца, сначала необходимо сбросить его с помощью команды **no sflow receiver**. Получатель будет отключен после окончания его срока действия, а запись получателя вернется к настройкам по умолчанию. Таймер истечения срока записи начинает обратный отсчет после настройки его значения. Пользователь не может указать «0» в качестве значения таймера истечения срока записи.

Пример

В данном примере показано, как настроить получателя с индексом 1. Имя владельца – collector1. Значение тайм-аута – 86400 секунд. Размер – 1400 байтов. IP-адрес удаленного получателя sFlow – 10.1.1.2. Номер порта – 6343.

```
Switch# configure terminal
Switch(config)# sflow receiver 1 owner collector1 expiry 86400 max-datagram-size 1400 host
10.1.1.2 udp-port 6343
Switch(config)#
```

80-2 sflow sampler

Данная команда используется для создания или настройки выборки для агента sFlow. Используйте форму **no**, чтобы удалить одну выборку.

sflow sampler *INSTANCE* [**receiver** *RECEIVER*] [**inbound** | **outbound**] [**sampling-rate** *RATE*][**max-header-size** *SIZE*]
no sflow sampler *INSTANCE*

Параметры

<i>INSTANCE</i>	Укажите индекс экземпляра, если с одним интерфейсом ассоциировано несколько выборок. Доступный диапазон значений: от 1 до 65535.
receiver <i>RECEIVER</i>	(Опционально) Укажите индекс получателя указанной выборки. Если параметр не указан, значение равно нулю. Пользователь не может указать «0» в качестве данного значения.
inbound	(Опционально) Укажите для выборки входящих пакетов. По умолчанию используется данное направление выборки.
outbound	(Опционально) Укажите для выборки исходящих пакетов.
sampling-rate <i>RATE</i>	(Опционально) Укажите частоту выборки пакетов. Доступный диапазон значений: от 0 до 65536. Если параметр не указан или указан «0», выборка будет отключена.
max-header-size <i>SIZE</i>	(Опционально) Укажите максимальное количество байтов, которое необходимо скопировать из пакетов выборки. Доступный диапазон значений: от 18 до 256. Если параметр

не указан, значение по умолчанию составляет 128.

По умолчанию

По умолчанию ни одной выборки не создано.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду без ключевых слов, чтобы создать выборку по умолчанию или вернуть значения по умолчанию для существующей выборки. При использовании формы по укажите индекс экземпляра выборки, которую необходимо удалить.

Пользователь может указать только получателя, для которого настроено имя владельца. Если имя владельца получателя сброшено, ассоциированная с ним выборка вернется к настройкам по умолчанию. ID получателя выборки по умолчанию составляет 0.

Возможна настройка двух режимов для экземпляра: inbound или outbound. Если режим не указан, по умолчанию используется inbound, который применяется для контроля входящих пакетов.

На интерфейсе возможна настройка нескольких выборок. Настроенная частота нескольких выборок может отличаться, но частота всех других выборок в одном направлении должна быть кратна минимальной настроенной частоте выборки во второй степени.

Во время перегрузки системы текущая частота выборки может быть автоматически понижена.

Пример

В данном примере показано, как создать выборку экземпляра 1. Получатель – 1. Режим – inbound. Частота – 1024. Размер – 128 байтов.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# sflow sampler 1 receiver 1 inbound sampling-rate 1024 max-header-size 128
Switch(config-if)#
```

80-3 sflow poller

Данная команда используется для создания или настройки опроса для агента sFlow. Используйте форму **no**, чтобы удалить опрос.

sflow poller *INSTANCE* [**receiver** *RECEIVER*] [**interval** *SECONDS*]
no sflow poller *INSTANCE*

Параметры

INSTANCE

Укажите индекс экземпляра, если с одним интерфейсом

	ассоциировано несколько опросов. Доступный диапазон значений: от 1 до 65535.
receiver <i>RECEIVER</i>	(Опционально) Укажите индекс получателя указанного опроса. Если параметр не указан, значение равно нулю. Пользователь не может указать «0» в качестве данного значения.
interval <i>SECONDS</i>	(Опционально) Укажите максимальное количество секунд между последовательными выборками опроса. Доступный диапазон значений: от 0 до 120. Если параметр не указан или указан «0», опрос будет отключен.

По умолчанию

Опросы по умолчанию не созданы.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду без ключевых слов, чтобы создать опрос по умолчанию или вернуть значения по умолчанию для существующего опроса. При использовании формы по укажите индекс экземпляра опроса, который необходимо удалить.

Пользователь может указать только выборку, для которого настроено имя владельца. Если имя владельца получателя сброшено, ассоциированный с ним опрос вернется к настройкам по умолчанию.

Если для интервала опроса установлено значение 0, опрос будет отключен. На интерфейсе может быть установлено несколько опросов.

Пример

В данном примере показано, как создать опрос экземпляра 1. Получатель – 1. Интервал – 20 секунд.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# sflow poller 1 receiver 1 interval 20
Switch(config-if)#
```

80-4 show sflow

Данная команда используется для отображения информации об sFlow.

show sflow [agent | receiver | sampler | poller]

Параметры

agent	(Опционально) Укажите для отображения информации об
--------------	---

	агенте sFlow.
receiver	(Опционально) Укажите для отображения информации о всех получателях.
sampler	(Опционально) Укажите для отображения информации о всех выборках.
poller	(Опционально) Укажите для отображения информации о всех опросах.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию об sFlow. При отсутствии поддержки MIB, строка sFlow Agent Version с указанием версии MIB будет пустой. При изменении vendor имя организации в строке sFlow Agent Version также будет изменено.

Пример

В данном примере показано, как отобразить информацию о всех типах объектов sFlow.

```

Switch#show sflow

sFlow Agent Version      : 1.3;D-Link Corporation Inc.;1.00
sFlow Agent Address     : 10.90.90.91
sFlow Agent IPv6 Address :

Receivers Information

Index                    : 1
Owner                   :
Expire Time             : 0
Current Countdown Time  : 0
Max Datagram Size      : 1400
Address                 : 0.0.0.0
Port                   : 6343
Datagram Version       : 5

Index                    : 2
Owner                   :
Expire Time             : 0
Current Countdown Time  : 0
Max Datagram Size      : 1400
Address                 : 0.0.0.0
Port                   : 6343
Datagram Version       : 5

Index                    : 3
Owner                   :
Expire Time             : 0
Current Countdown Time  : 0
Max Datagram Size      : 1400
Address                 : 0.0.0.0
Port                   : 6343
Datagram Version       : 5

Index                    : 4
Owner                   :
Expire Time             : 0
Current Countdown Time  : 0
Max Datagram Size      : 1400
Address                 : 0.0.0.0
Port                   : 6343
Datagram Version       : 5

Samplers Information
Interface Instance Receiver  Mode   Admin Rate  Active Rate  Max Header Size
-----
Pollers Information
Interface Instance Receiver Interval
-----

Switch#
    
```

Отображаемые параметры

sFlow Agent Version	Версия MIB, организация и версия программного обеспечения.
----------------------------	--

sFlow Agent Address	IPv4-адрес агента sFlow.
sFlow Agent IPv6 Address	IPv6-адрес агента sFlow.
Index	Индекс получателей.
Owner	Имя владельца.
Expire Time	Время истечения срока записи, настроенное пользователем.
Current Countdown Time	Время (в секундах), оставшееся до прекращения выборки и опроса.
Max Datagram Size	Максимальное количество байтов одной дейтаграммы sFlow.
Address	IPv4/IPv6-адрес удаленного получателя sFlow.
Port	UDP-порт удаленного получателя sFlow.
Datagram Version	Версия дейтаграммы sFlow.
Interface	Интерфейс, на котором настроена выборка.
Instance	Индекс экземпляра выборки.
Receiver	Индекс получателя для указанной выборки.
Mode	Режимы для экземпляров: inbound, outbound и inactive.
Admin Rate	Частота для выборки пакетов, настроенная пользователем.
Max Header Size	Максимальное количество байтов, которое необходимо скопировать из пакетов выборки.
Interface	Интерфейс, на котором настроен опрос
Instance	Индекс экземпляра опроса.
Receiver	Индекс получателя для указанного опроса.
Interval	Максимальное количество секунд между последовательными опросами.

81. Команды Simple Mail Transfer Protocol (SMTP)

81-1 smtp server

Данная команда используется для настройки SMTP-сервера и порта.

```
smtp server {IP-ADDRESS | IPV6-ADDRESS} [port PORT]no smtp server [port]
```

Параметры

<i>IP-ADDRESS</i>	Укажите IPv4-адрес SMTP-сервера.
<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес SMTP-сервера.
<i>PORT</i>	Укажите номер TCP-порта для подключения к SMTP-серверу. Доступный диапазон значений: от 1 до 65535.

По умолчанию

По умолчанию адрес сервера не настроен.
Номер порта по умолчанию – 25.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Система обеспечивает сервис для отправки syslog-сообщений получателям по электронной почте через SMTP. Для отправки сообщений по электронной почте необходимо настроить почтовый сервер, получателя и собственный адрес почты. Коммутатор, выступающий в роли SMTP-клиента, отправляет syslog-сообщения на SMTP-сервер, с которого сообщения по электронной почте передаются получателю. На коммутаторе может быть настроен только один SMTP-сервер.

Пример

В данном примере показано, как настроить IP-адрес сервера и TCP-порт. IP-адрес сервера – 172.18.208.9. TCP-порт – 587.

```
Switch# configure terminal
Switch(config)# smtp server 172.18.208.9 port 587
Switch(config)#
```

81-2 smtp self

Данная команда используется для настройки адреса электронной почты коммутатора для отправки сообщений по электронной почте. Используйте форму **no**, чтобы удалить адрес электронной почты коммутатора.

smtp self *EMAIL-ADDRESS*
no smtp self

Параметры

self <i>EMAIL-ADDRESS</i>	Укажите адрес электронной почты коммутатора.
----------------------------------	--

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить адрес электронной почты коммутатора. На коммутаторе может быть настроен только один адрес электронной почты.

Пример

В данном примере показано, как настроить адрес электронной почты отправителя для коммутатора. Настроенный адрес – switch@domain.com.

```
Switch# configure terminal
Switch(config)# smtp self switch@domain.com
Switch(config)#
```

81-3 smtp recipient

Данная команда используется для настройки получателя электронных писем. Используйте форму **no**, чтобы удалить получателя.

smtp recipient *EMAIL-ADDRESS*
no smtp recipient {all | *EMAIL-ADDRESS*}

Параметры

<i>EMAIL-ADDRESS</i>	Укажите получателя электронных писем.
all	Укажите, чтобы удалить всех получателей.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Система обеспечивает сервис для отправки syslog-сообщений получателям по электронной почте через SMTP. Чтобы получать сообщения по электронной почте, необходимо настроить адрес электронной почты при помощи команды **smtp recipient**. По умолчанию отправка сообщений не включена. Чтобы разрешить отставку syslog-сообщений получателям по электронной почте и настроить критерии фильтрации, используйте команду **logging smtp**.

Пример

В данном примере показано, как добавить адрес электронной почты получателя. Добавленный адрес – receiver@domain.com.

```
Switch# configure terminal
Switch(config)# smtp recipient receiver@domain.com
Switch(config)#
```

81-4 smtp interval

Данная команда используется для настройки SMTP-интервала. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

smtp interval MINUTES
no smtp interval

Параметры

<i>MINUTES</i>	Укажите интервал отправки SMTP. Если указан 0, сообщение о каждом событии будет отправляться коммутатором немедленно.
----------------	---

По умолчанию

Значение по умолчанию – 30 минут.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить интервал отправки SMTP для коммутатора.

Пример

В данном примере показано, как настроить интервал в 10 минут.

```
Switch# configure terminal
Switch(config)# smtp interval 10
Switch(config)#
```

81-5 show smtp

Данная команда используется для отображения информации об SMTP.

show smtp

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию об SMTP.

Пример

В данном примере показано, как отобразить информацию об SMTP.

```
Switch#show smtp

SMTP IPv4 Server Address: 172.18.50.9
SMTP IPv4 Server Port   : 25
SMTP IPv6 Server Address: 2000::91
SMTP IPv6 Server Port   : 65535
Self Mail Address       : switch@domain.com
Send Interval           : 0

Index   Mail Receiver Address
-----
1       receiver1@domain.com
2       receiver2@domain.com
3       receiver3@domain.com
4       receiver4@domain.com
5       receiver5@domain.com
6       receiver6@domain.com
7       receiver7@domain.com
8       receiver8@domain.com
Switch#
```

81-6 smtp send-testmsg

Данная команда используется для проверки доступности SMTP-сервера.

smtp send-testmsg

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы проверить доступность SMTP-сервера. Электронные письма отправляются всем настроенным получателям.

Пример

В данном примере показано, как отправить тестовое письмо всем пользователям, которые находятся в текущем настроенном списке получателей.

```
Switch# smtp send-testmsg  
  
Subject: This is the test message subject!  
Content: This is the test message content!  
  
Sending mail, please wait!  
  
Switch#
```

82. Команды протокола Simple Network Management Protocol (SNMP)

82-1 show snmp

Данная команда используется для отображения настроек SNMP.

```
show snmp {community | host | view | group | engineID}
```

Параметры

community	Укажите, чтобы отобразить информацию об SNMP-сообществе.
host	Укажите, чтобы отобразить информацию о получателе SNMP trap.
view	Укажите, чтобы отобразить информацию об SNMP View.
group	Укажите, чтобы отобразить информацию об SNMP-группе.
engineID	Укажите, чтобы отобразить информацию о SNMP local engine ID.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Любой режим конфигурации

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для отображения информации об SNMP. При отображении строк SNMP Community String созданные SNMPv1 или SNMPv2c-пользователи не будут отображены.

Пример

В данном примере показано, как отобразить информацию об SNMP-сообществе.

```
Switch#show snmp community

Community : public
Access : read-only
View : CommunityView

Community : private
Access : read-write
View : CommunityView

Total Entries: 2

Switch#
```

В данном примере показано, как отобразить настройки SNMP-сервера.

```
Switch#show snmp host

Host IP Address : 10.90.90.1
SNMP Version : V1
Community Name : public
UDP Port : 162

Total Entries: 1

Switch#
```

В данном примере показано, как отобразить настройки MIB View.

```
Switch#show snmp view

restricted(included) 1.3.6.1.2.1.1
restricted(included) 1.3.6.1.2.1.11
restricted(included) 1.3.6.1.6.3.10.2.1
restricted(included) 1.3.6.1.6.3.11.2.1
restricted(included) 1.3.6.1.6.3.15.1.1
CommunityView(included) 1
CommunityView(excluded) 1.3.6.1.6.3
CommunityView(included) 1.3.6.1.6.3.1

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
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

В данном примере показано, как отобразить SNMP engine ID.

```
Switch#show snmp engineID

Local SNMP engineID: 800000ab03f07d6834001000

Switch#
```

82-2 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

Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 12

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

User Name: initial
Security Model: 3
Group Name: initial
Authentication Protocol: None
Privacy Protocol: None
Engine ID: 800000ab03f07d6834001000
IP access control list:

Total Entries: 1

Switch#
```

82-3 snmp-server community

Данная команда используется для настройки строки идентификатора сообщества (Community String) для доступа к SNMP. Используйте форму **no**, чтобы удалить строку Community String.

```
snmp-server community [0 | 7] COMMUNITY-STRING [view VIEW-NAME] [ro | rw] [access IP-ACL-NAME]
[context CONTEXT]
no snmp-server community [0 | 7] COMMUNITY-STRING
```

Параметры

0 <i>COMMUNITY-STRING</i>	(Опционально) Укажите строку Community String в форме обычного текста. Максимально допустимое количество символов в строке – 32. Данное значение используется по умолчанию.
7 <i>COMMUNITY-STRING</i>	(Опционально) Укажите строку Community String в зашифрованном виде.
view <i>VIEW-NAME</i>	(Опционально) Укажите имя ранее настроенного View, которое доступно указанному SNMP-сообществу.
ro	(Опционально) Укажите право «только чтение».
rw	(Опционально) Укажите право «чтение/запись».
access <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.
context <i>CONTEXT</i>	(Опционально) Укажите имя SNMP-контекста.

По умолчанию

Community	View Name	Access right
private	CommunityView	Read/Write (чтение/запись)
public	CommunityView	Read Only (только чтение)

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Данная команда предоставляет простой способ для создания строки Community String для управления SNMPv1 и SNMPv2c. При создании сообщества с помощью команды **snmp-server community** будут созданы две записи SNMP-группы: одна для SNMPv1 и другая для SNMPv2c, у которых имя сообщества совпадают с именами групп. Если View не указан, разрешен доступ ко всем объектам.

Пример

В данном примере показано, как создать MIB View «interfacesMibView» и строку Community String «comaccess», с помощью которой можно получить право «чтение/запись» к созданному View «interfacesMibView».

```
Switch# configure terminal
Switch(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)# snmp-server community comaccess view interfacesMibView rw
Switch(config)#
```

82-4 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

Уровень команды по умолчанию

Уровень 15

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 33220000000000000000000000000000.

```
Switch# configure terminal
Switch(config)# snmp-server engineID local 3322
Switch(config)#
```

82-5 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.
v1	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv1.
v2c	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv2c.
v3	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv3.
auth	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv3.
noauth	Укажите для отмены аутентификации и шифрования пакетов.
priv	Укажите для аутентификации и шифрования пакетов.
read <i>READ-VIEW</i>	(Опционально) Укажите, чтобы обеспечить доступ на чтение пользователю данной группы.
write <i>WRITE-VIEW</i>	(Опционально) Укажите, чтобы обеспечить доступ на запись пользователю данной группы.
notify <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.
access IP-ACL-NAME	(Опционально) Укажите стандартный IP-адрес списка управления доступом (ACL) для ассоциирования с группой.

По умолчанию

Group Name	Version	Security Level	Read View Name	Write View Name	Notify View
Initial	SNMPv3	noauth	Restricted	None	Restricted
ReadGroup	SNMPv1	noauth	CommunityView	None	CommunityView
ReadGroup	SNMPv2c	noauth	CommunityView	None	CommunityView
WriteGroup	SNMPv1	noauth	CommunityView	CommunityView	CommunityView
WriteGroup	SNMPv2c	noauth	CommunityView	CommunityView	CommunityView

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Для определения пользователя SNMP-группы необходимо указать разрешенную модель безопасности и право с помощью параметров *READ-VIEW*, *WRITE-VIEW* и *NOTIFY-VIEW*. Модель безопасности позволяет пользователю использовать указанную версию SNMP при доступе к агенту SNMP.

Возможно создание групп с одинаковыми именами при указании разных моделей безопасности SNMPv1, SNMPv2c и SNMPv3 одновременно. При указании SNMPv3 доступно использование двух параметров **auth** и **priv** одновременно.

Чтобы загрузить новый профиль View для группы для определенной модели безопасности, удалите ранее созданную группу и создайте новую группу с новым профилем View.

Параметр *READ-VIEW* определяет MIB-объекты, которые доступны для чтения пользователю группы. Если *READ-VIEW* не указан, может быть прочитано Internet OID-пространство 1.3.6.1.

Параметр *WRITE-VIEW* определяет MIB-объекты, которые доступны для записи пользователю группы. Если *WRITE-VIEW* не указан, никакой из MIB-объектов не может быть записан.

Параметр *NOTIFY-VIEW* определяет MIB-объекты, с помощью которых система может сообщать о своем статусе в notify-пакетах уведомлений trap-менеджерам, которые идентифицированы указанным пользователем группы, выступающим в качестве строки Community String. Если *NOTIFY-VIEW* не указан, информация о MIB-объектах не будет получена.

Пример

В данном примере показано, как создать группу SNMP-сервера для доступа по SNMPv3 и SNMPv2c. Настроенная группа – guestgroup.

```
Switch# configure terminal
Switch(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)# snmp-server group guestgroup v3 auth read interfacesMibView
Switch(config)# snmp-server group guestgroup v2c read CommunityView write CommunityView
Switch(config)#
```

82-6 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.
version	(Опционально) Укажите версию SNMP, которую необходимо использовать для отправки SNMP trap. Если версия не указана, по умолчанию используется SNMPv1. 1 – SNMPv1. 2c – SNMPv2c. 3 – SNMPv3.
auth	(Опционально) Укажите для аутентификации пакетов. Данный параметр не используется для шифрования пакетов.
noauth	Укажите для отмены аутентификации и шифрования пакетов.
priv	Укажите для аутентификации и шифрования пакетов.
<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 snmp-sever user .
port <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

Уровень команды по умолчанию

Уровень 15

Использование команды

SNMP-уведомления отправляются в виде SNMP trap. Для отправки SNMP-уведомлений необходимо создать по крайней мере одного получателя при помощи команды **snmp-server host**. Для созданного пользователя укажите версию SNMP trap-пакетов. При указании SNMPv1 и SNMPv2c уведомления SNMP trap будут отправлены в PDU (Trap Protocol Data Unit). При указании SNMPv3 уведомления SNMP trap будут отправлены в SNMPv2-TRAP-PDU с заголовком SNMPv3.

При указании SNMPv1 или SNMPv2c для отправки SNMP trap на определенный узел указанная строка Community String выступает в качестве строки SNMP trap.

При указании SNMPv3 для отправки SNMP trap на определенный узел укажите, необходима ли аутентификация и шифрование отправленных пакетов. Указанная строка Community String выступает в качестве имени пользователя в пакетах SNMPv3. При использовании команд **snmp-server user** или **snmp-server user v3** сначала необходимо создать пользователя.

При отправке SNMP trap система проверит уведомления View, ассоциированные с указанным пользователем или именем сообщества. Если 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)#
```

82-7 snmp-server source-interface traps

Данная команда используется для указания интерфейса, IP-адрес которого будет использован в качестве адреса источника для отправки пакетов SNMP trap. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
snmp-server source-interface traps INTERFACE-ID  
no snmp-server source-interface traps
```

Параметры

<i>INTERFACE-ID</i>	Укажите интерфейс, IP-адрес которого будет использован в качестве адреса источника для отправки пакетов SNMP trap.
---------------------	--

По умолчанию

По умолчанию используется IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для указания интерфейса, IP-адрес которого будет использован в качестве адреса источника для отправки пакетов SNMP trap.

Пример

В данном примере показано, как настроить VLAN 100 в качестве интерфейса источника для отправки пакетов SNMP trap.

```
Switch# configure terminal  
Switch(config)# snmp-server source-interface traps vlan 100  
Switch(config)#
```

82-8 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 {des PRIV-PASSWORD | aes 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.
v1	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv1.
v2c	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv2c.
v3	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv3.
encrypted	(Опционально) Укажите для шифрования пароля.
auth	(Опционально) Укажите тип аутентификации.
md5	(Опционально) Укажите использование аутентификации MAC-MD5-96.
sha	(Опционально) Укажите использование аутентификации HMAC-SHA-96.
<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 encrypted длина пароля для MD5 составляет 32, для SHA – 40. В данном параметре используются шестнадцатеричные значения.
priv	(Опционально) Укажите тип шифрования.
des	(Опционально) Укажите использование алгоритма DES для шифрования.
aes	(Опционально) Укажите использование алгоритма AES для шифрования.
<i>PRIV-PASSWORD</i>	Укажите пароль Private в форме обычного текста. Максимально допустимое количество символов – 64. При указании параметра encrypted фиксированная длина пароля – 16 символов.
access IP-ACL-NAME	(Опционально) Укажите стандартный IP-адрес ACL для ассоциирования с пользователем.

По умолчанию

По умолчанию настроен один пользователь.

Имя пользователя – initial.

Имя группы – initial.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Для создания SNMP-пользователя укажите модель безопасности, которая будет использована данным пользователем, и группу, для которой создан данный пользователь. Для создания SNMPv3-пользователя необходимо указать пароль для аутентификации и шифрования.

Невозможно удалить SNMP-пользователя, который был ассоциирован с SNMP-сервером.

Пример

В данном примере показано, как настроить пароль в форме обычного текста для пользователя «user1» в группе «public» в версии SNMPv3.

```
Switch# configure terminal
Switch(config)# snmp-server user user1 public v3 auth md5 authpassword priv privpassword
Switch(config)#
```

В данном примере показано, как использовать строку MD5 digest вместо пароля в форме обычного текста.

```
Switch# configure terminal
Switch(config)# snmp-server user user1 public v3 encrypted auth md5
00112233445566778899AABBCCDDEEFF
Switch(config)#
```

82-9 snmp-server view

Данная команда используется для создания или изменения записи View. Используйте форму no, чтобы удалить указанную запись SNMP View.

snmp-server view *VIEW-NAME* *OID-TREE* {**included** | **excluded**}
no snmp-server view *VIEW-NAME*

Параметры

<i>VIEW-NAME</i>	Укажите имя записи View. Доступный диапазон значений: от 1 до 32 символов. Пробелы в строке недопустимы.
<i>OID-TREE</i>	Укажите идентификатор объекта (Object Identifier, OID) под-дерева ASN.1, который необходимо включить или исключить из View. Для идентификации под-дерева введите строку, состоящую либо из чисел, например, 1.3.6.2.4, либо из слов, например, system. При указании семейства под-деревьев используйте подстановочный знак (*) перед каждым идентификатором под-дерева.
included	Укажите под-дерево, которое необходимо включить в SNMP View.
excluded	Укажите под-дерево SNMPv1, которое необходимо исключить из SNMP View.

По умолчанию

VIEW-NAME	OID-TREE	View Type
Restricted	1.3.6.1.2.1.1	Included
Restricted	1.3.6.1.2.1.11	Included
Restricted	1.3.6.1.6.3.10.2.1	Included
Restricted	1.3.6.1.6.3.11.2.1	Included

Restricted	1.3.6.1.6.3.15.1.1	Included
CommunityView	1	Included
CommunityView	1.3.6.1.6.3	Excluded
CommunityView	1.3.6.1.6.3.1	Included

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы создать View MIB-объектов.

Пример

В данном примере показано, как создать MIB View и предоставить доступ для чтения SNMP-группе, ассоциированной с данным MIB View. Настроенный MIB View – interfacesMibView. SNMP-группа – guestgroup.

```
Switch# configure terminal
Switch(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)# snmp-server group guestgroup v3 auth read interfacesMibView
Switch(config)#
```

82-10 show snmp trap link-status

Данная команда используется для отображения состояния trap-статуса состояния линии связи (link- status) на интерфейсе.

show snmp trap link-status [interface *INTERFACE-ID* [, | -]]

Параметры

interface <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

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения состояния trap-статуса при обнаружении/разрыве соединения состояния link-up/link-down на интерфейсе.

Пример

В данном примере показано, как отобразить trap-статус состояния link-up/link-down для диапазона интерфейсов от Ethernet 1/0/1 до Ethernet 1/0/9.

```
Switch#show snmp trap link-status interface ethernet 1/0/1-9

Interface          Trap state
-----
eth1/0/1           Enabled
eth1/0/2           Enabled
eth1/0/3           Enabled
eth1/0/4           Enabled
eth1/0/5           Enabled
eth1/0/6           Enabled
eth1/0/7           Enabled
eth1/0/8           Enabled
eth1/0/9           Enabled

Switch#
```

82-11 show snmp-server

Данная команда используется для отображения глобальных настроек о состоянии SNMP-сервера и настроек, касающихся состояния trap.

show snmp-server [traps]

Параметры

traps	(Опционально) Укажите для отображения настроек, касающихся состояния trap.
--------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Для отображения глобальных настроек о состоянии SNMP-сервера используйте команду **show snmp-server**.

Для отображения настроек, касающихся состояния trap, используйте команду **show snmp-server traps**.

Пример

В данном примере показано, как отобразить настройки SNMP-сервера.

```
Switch#show snmp-server

SNMP Server   : Enabled
Name          : Switch
Location      :
Contact       :
SNMP UDP Port : 161
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            : Disabled
  Warmstart            : Disabled

Switch#
```

82-12 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 командыUser/Privileged EXEC Mode
Любой режим конфигурации**Уровень команды по умолчанию**

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить состояние отправки SNMP trap на порту. Если ни один из опциональных параметров не указан, будут отображены все порты.

Пример

В данном примере показано, как отобразить состояние отправки SNMP trap для диапазона интерфейсов от Ethernet 1/0/1 до Ethernet 1/0/9.

```
Switch#show snmp-server trap-sending interface ethernet 1/0/1-9
```

Port	Trap Sending
eth1/0/1	Enabled
eth1/0/2	Enabled
eth1/0/3	Enabled
eth1/0/4	Enabled
eth1/0/5	Enabled
eth1/0/6	Enabled
eth1/0/7	Enabled
eth1/0/8	Enabled
eth1/0/9	Enabled

```
Switch#
```

82-13 snmp-server

Данная команда используется для включения агента SNMP. Используйте форму **no**, чтобы выключить агента SNMP.

```
snmp-server
no snmp-server
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Менеджер SNMP управляет агентом SNMP: отправляет SNMP-запросы агенту и получает ответы и SNMP-уведомления от агента. Для управления агентом необходимо включить на нем SNMP-сервер.

Пример

В данном примере показано, как включить SNMP-сервер.

```
Switch# configure terminal
Switch(config)# snmp-server
Switch(config)#
```

82-14 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить системную контактную информацию для управления устройством.

Пример

В данном примере показано, как указать строку с системной контактной информацией. Указанная строка – MIS Department II.

```
Switch# configure terminal
Switch(config)# snmp-server contact MIS Department II
Switch(config)#
```

82-15 snmp-server enable traps

Данная команда используется для глобального включения отправки SNMP trap. Используйте форму **no**, чтобы отключить отработку SNMP trap.

snmp-server enable traps
no snmp-server enable traps

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить отработку SNMP trap глобально на устройстве.

Пример

В данном примере показано, как включить отработку SNMP trap глобально.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps
Switch(config)#
```

82-16 snmp-server enable traps snmp

Данная команда используется для включения отправки всех или определенных SNMP-уведомлений. Используйте форму **no**, чтобы отключить отработку всех или определенных SNMP-уведомлений.

snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]
no snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]

Параметры

authentication	(Опционально) Укажите для отправки SNMP trap об ошибке аутентификации. Trap-сообщение «authenticationFailuretrap» генерируется, если устройство получает SNMP-сообщение, которое не аутентифицировано должным образом. Метод аутентификации зависит от используемой версии SNMP. При использовании SNMPv1 или SNMPv2c ошибка аутентификации возникает, если пакеты были сформированы с указанием неверной строки Community String. При использовании SNMPv3 ошибка аутентификации возникает, если пакеты были сформированы с указанием неверного ключа аутентификации SHA/MD5.
linkup	(Опционально) Укажите для отправки SNMP-уведомлений об установленном соединении. Trap-сообщение «linkUp (3)» генерируется, если на устройстве установлено соединение хотя бы с одним из каналов связи.
linkdown	(Опционально) Укажите для отправки SNMP-уведомлений о прерванном соединении. Trap-сообщение «linkDown (2)» генерируется, если на устройстве прервано соединение хотя бы с одним из каналов связи.
coldstart	(Опционально) Укажите для отправки SNMP-уведомлений о «холодном» старте.
warmstart	(Опционально) Укажите для отправки SNMP-уведомлений о «горячем» старте.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для управления отправкой стандартных SNMP trap. Чтобы включить отправку SNMP-trap, необходимо также включить этот параметр глобально.

Пример

В данном примере показано, как включить отправку всех SNMP trap на узел 10.9.18.100, используя строку сообщества «public».

```
Switch# configure terminal
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server enable traps snmp
Switch(config)# snmp-server host 10.9.18.100 version 2c public
Switch(config)#
```


В данном примере показано, как включить SNMP trap об ошибке аутентификации.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps snmp authentication
Switch(config)#
```

82-17 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для указания информации о системном местоположении на коммутаторе.

Пример

В данном примере показано, как указать строку с информацией о системном местоположении. Указанная строка – HQ 15F.

```
Switch# configure terminal
Switch(config)# snmp-server location HQ 15F
Switch(config)#
```

82-18 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для указания информации о системном имени коммутатора.

Пример

В данном примере показано, как настроить системное имя. Настроенное имя – SiteA-switch.

```
Switch# configure terminal
Switch(config)# snmp-server name SiteA-switch
Switch(config)#
```

82-19 snmp-server trap-sending disable

Данная команда используется для отключения отправки SNMP trap на порту. Используйте форму **no**, чтобы включить отработку SNMP trap на порту.

```
snmp-server trap-sending disable
no snmp-server trap-sending disable
```

Параметры

Нет

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для отключения отправки сгенерированных системой SNMP trap с определенного порта. Данная команда не применима для SNMP trap, сгенерированных другой системой и переадресованных на порт.

Пример

В данном примере показано, как отключить отставку 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)#
```

82-20 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для настройки номера UDP-порта SNMP на коммутаторе. Агент будет прослушивать пакеты SNMP Request на сервисном UDP-порту настроенного номера.

Пример

В данном примере показано, как настроить номер UDP-порта SNMP.

```
Switch# configure terminal
Switch(config)# snmp-server service-port 50000
Switch(config)#
```

82-21 snmp-server response broadcast-request

Используйте данную команду, чтобы разрешить серверу отвечать на широковещательные пакеты SNMP GetRequest. Используйте форму **no**, чтобы запретить серверу отвечать на широковещательные пакеты SNMP GetRequest.

```
snmp-server response broadcast-request  
no snmp-server response broadcast-request
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы разрешить серверу отвечать на широковещательные пакеты SNMP GetRequest, которые будут отправлены средствами NMS для определения сетевого устройства. Для применения данной функции необходимо включить ответ на широковещательные пакеты GetRequest.

Пример

В данном примере показано, как разрешить серверу отвечать на широковещательные пакеты SNMP GetRequest.

```
Switch# configure terminal  
Switch(config)# snmp-server response broadcast-request  
Switch(config)#
```

82-22 snmp trap link-status

Данная команда используется для включения отправки уведомлений об обнаружении/разрыве соединения (link-up/link-down), произошедшего на интерфейсе. Используйте форму **no**, чтобы отключить отправку.

```
snmp trap link-status  
no snmp trap link-status
```

Параметры

Нет

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения или отключения отправки SNMP trap об обнаружении/разрыве соединения (link-up/link-down) на интерфейсе.

Пример

В данном примере показано, как отключить отставку 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)#
```

83. Команды Single IP Management (SIM)

83-1 sim

Данная команда используется для включения функции Single IP Management. Используйте форму **no**, чтобы отключить функцию Single IP Management.

sim
no sim

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для включения/отключения функции Single IP Management на устройстве.

Пример

В данном примере показано, как включить Single IP Management.

```
Switch# configure terminal
Switch(config)# sim
Switch(config)#
```

83-2 sim role

Данная команда используется для смены роли Candidate Switch на Commander Switch или Commander Switch на Candidate Switch.

sim role {commander [GROUP-NAME] | candidate}

Параметры

commander	Укажите для передачи роли Commander Switch устройству.
<i>GROUP-NAME</i>	(Опционально) Укажите имя группы, назначая устройству роль Commander Switch.
candidate	Укажите для передачи роли Candidate Switch устройству.

По умолчанию

Имя группы Single IP Management по умолчанию – default.

Роль устройства по умолчанию – Candidate Switch.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Технология Single IP Management предусматривает три роли: Candidate Switch и Commander Switch (назначаются пользователем), а также Member Switch (назначается при помощи команды **sim group- member** на Commander Switch).

В SIM-группу входит Commander Switch и множество Member Switch. При смене роли устройства, например, с Commander Switch на Candidate Switch все роли участников SIM-группы будут изменены на Candidate Switch.

Пример

В данном примере показано, как создать SIM-группу.

```
Switch# configure terminal
Switch(config)# sim role commander my-group
Switch(config)#
```

83-3 sim group-member

Данная команда используется для добавления одного Candidate Switch в SIM-группу. Используйте форму **no**, чтобы удалить одного участника из данной SIM-группы.

```
sim group-member CANDIDATE-ID [PASSWORD]
no sim group-member MEMBER-ID
```

Параметры

<i>CANDIDATE-ID</i>	Укажите одно устройство в роли Candidate Switch в одной SIM-группе.
<i>PASSWORD</i>	(Опционально) Укажите пароль устройства в роли Candidate Switch.
<i>MEMBER-ID</i>	Укажите одно устройство в роли Member Switch в одной SIM-группе.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

После того как Candidate Switch пройдет аутентификацию 15-уровневого пароля, Commander Switch позволит данному Candidate Switch присоединиться к SIM-группе в качестве Member Switch.

Пример

В данном примере показано, как добавить один Candidate Switch к SIM-группе.

```
Switch# configure terminal
Switch(config)# sim group-member 1 secret
Switch(config)#
```

83-4 sim holdtime

Данная команда используется для настройки времени в секундах параметра Hold-Time. Если устройство (Commander Switch или Candidate Switch) по истечении данного времени не получит сообщения Single IP Management, информация о другом устройстве будет удалена. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
sim holdtime SECONDS
no sim holdtime
```

Параметры

SECONDSУкажите значение параметра Hold-Time. Доступный диапазон значений: от 100 до 255 секунд.

По умолчанию

Значение по умолчанию – 100 секунд.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если в течение указанного Hold-Time устройство в роли Commander Switch не получит ни одного сообщения протокола SIM, информация о Member Switch будет удалена. Если сообщения не получит Member Switch, будет удалена информация о Commander Switch, роль которого будет изменена на Candidate Switch.

Пример

В данном примере показано, как настроить параметр SIM Hold-Time.

```
Switch# configure terminal
Switch(config)# sim holdtime 120
Switch(config)#
```

83-5 sim interval

Данная команда используется для настройки SIM-интервала в секундах для отправки сообщений протокола Single IP Management. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

sim interval SECONDS
no sim interval

Параметры

SECONDSУкажите значение интервала. Доступный диапазон значений: от 30 до 90 секунд.

По умолчанию

Значение по умолчанию – 30 секунд.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить SIM-интервал в секундах для отправки сообщений протокола Single IP Management.

Пример

В данном примере показано, как настроить интервал для протокола Single IP Management.

```
Switch# configure terminal
Switch(config)# sim interval 60
Switch(config)#
```

83-6 sim management vlan

Данная команда используется для настройки SIM Management VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
sim management vlan VLAN-ID
no sim management vlan
```

Параметры

VLAN-ID	Укажите ID SIM Management VLAN.
---------	---------------------------------

По умолчанию

Значение данного параметра по умолчанию – VLAN 1.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Commander Switch и Member Switch SIM-группы отправляют и получают сообщение SIM на SIM Management VLAN.

Пример

В данном примере показано, как настроить SIM Management VLAN. Настроенное значение – 100.

```
Switch# configure terminal
Switch(config)# sim management vlan 100
Switch(config)#
```

83-7 sim remote-config

Данная команда используется для удаленного входа в систему и настройки участника SIM-группы, а также для выхода из удаленной конфигурации.

sim remote-config {member MEMBER-ID | exit}

Параметры

member MEMBER-ID	Укажите логин участника.
exit	Укажите, чтобы выйти из текущей настраиваемой конфигурации участника.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Commander Switch может входить в учетную запись участников SIM-группы и настраивать их при помощи Member ID. Данная команда доступна только на Commander Switch.

Пример

В данном примере показано, как настроить Member ID.

```
Switch# sim remote-config member 1
Switch#
```

83-8 copy sim

Данная команда используется для копирования файлов участникам SIM-группы.

copy sim SOURCE-URL DESTINATION-URL [member MEMBER-LIST]

Параметры

SOURCE-URL	Укажите URL источника, который необходимо выгрузить на сервер. URL источника находится на Member Switch. Укажите текущую конфигурацию (Running Configuration) в качестве URL источника, чтобы выгрузить ее на TFTP-сервер. Укажите системный журнал (System Log) в качестве URL источника, чтобы выгрузить его на TFTP-сервер.
DESTINATION-URL	Укажите URL назначения для файла, который необходимо загрузить. URL назначения находится на Member Switch. Укажите текущую конфигурацию (Running Configuration) в качестве URL назначения, чтобы загрузить ее с TFTP-

	сервера на Member Switch. Укажите программное обеспечение (Firmware) в качестве URL назначения, чтобы загрузить его с TFTP-сервера на Member Switch. Загрузочный образ на Member Switch будет заменен загруженным файлом.
member MEMBER-LIST	(Опционально) Укажите Member Switch, чтобы загрузить файл. Может быть указано несколько Member Switch одновременно. Для отделения нескольких ID используйте «,»; для отделения диапазона interface ID используйте «-».

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Данная команда может использоваться на Commander Switch для выгрузки файлов с Member Switch на сервер. Для различия Member Switch ID каждому Member Switch ID будет добавлено имя файла.

Пример

В данном примере показано, как загрузить программное обеспечение (Firmware) на Member Switch 1.

```
Switch# copy sim tftp://10.10.10.58/switch.had firmware member 1

Download firmware 10.10.10.58/ switch.had to member 1 ?(y/n)(n) y

ID   MAC Address           Status
-----
1    00-02-01-03-01-03    SUCCESS

Switch#
```

В данном примере показано, как выгрузить системный журнал (System Log) с Member Switch 1.

```
Switch# copy sim system-log tftp: //10.10.10.58/switchlog member 1

Upload system log from member 1 to 10.10.10.58/switchlog ?(y/n)(n)y

ID   MAC Address           Status
-----
1    00-02-01-03-01-03    SUCCESS

Switch#
```

83-9 snmp-server enable traps sim

Данная команда используется для включения отправки trap-сообщений для SIM. Используйте форму **no**, чтобы отключить отправку.

snmp-server enable traps sim
no snmp-server enable traps sim

Параметры

Нет

По умолчанию

По умолчанию функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить/отключить отправку trap-сообщений для SIM.

Пример

В данном примере показано, как включить отправку trap-сообщений для SIM.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps sim
Switch(config)#
```

83-10 show sim

Данная команда используется для отображения информации о Single IP Management.

show sim [{**candidates** [*CANDIDATE-ID*] | **members** [*MEMBER-ID*] | **group** [*COMMANDER-MAC*] | **neighbor**}]

Параметры

candidates	(Опционально) Укажите, чтобы отобразить информацию обо всех Candidate Switch.
<i>CANDIDATE-ID</i>	(Опционально) Укажите, чтобы отобразить подробную информацию об одном определенном Candidate Switch.
members	(Опционально) Укажите, чтобы отобразить информацию обо всех Member Switch.
<i>MEMBER-ID</i>	(Опционально) Укажите, чтобы отобразить подробную информацию об одном определенном Member Switch.
group	(Опционально) Укажите, чтобы отобразить информацию о

	других SIM- группах.
COMMANDER-MAC	(Опционально) Укажите, чтобы отобразить подробную информацию об одной определенной группе.
neighbor	(Опционально) Укажите, чтобы отобразить информацию о соседних устройствах.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения информации о Single IP Management.

Пример

В данном примере показано, как отобразить подробную информацию о локальной SIM на Commander Switch.

```
Switch#show sim
Group Name       : my-group
SIM Version      : VER-1.61
Firmware Version : 1.00.001
Management VLAN  : 100
Device Name      : Switch
MAC Address      : F0-7D-68-36-30-B0
Platform         : DGS-3130-30TS
SIM State        : Enabled
Role State       : Commander
Discovery Interval : 60 sec
Hold Time        : 120 sec
Trap             : Enabled

Switch#
```

В данном примере показано, как отобразить подробную информацию о локальной SIM на Member Switch.

```
Switch# show sim

SIM Version       : VER-1.61
Firmware Version  : 1.00.001
Device Name       :
MAC Address       : F0-7D-00-36-30-B0
Platform         : DGS-3130-30TS
SIM State         : Enabled
Role State        : Member
Discovery Interval : 30 sec
Hold Time         : 100 sec

-----CS Info-----
CS Group Name     : my-group
CS MAC Address    : F0-7D-68-36-30-B0
CS Hold Time      : 90 s

Switch#
```

В данном примере показано, как отобразить список участников SIM-группы.

```
Switch# show sim members

Member
ID      MAC Address      Platform      Hold Time  Firmware Version  Device Name
-----
1       F0-7D-00-36-30-B0  DGS-3130-30TS  100       1.00.001
2       F0-7D-01-36-30-B0  DGS-3130-30TS   80       1.00.001

Total Entries : 2

Switch#
```

В данном примере показано, как отобразить подробную информацию об участнике SIM-группы.

```
Switch# show sim members 1

Sim Member Information :
Member ID              : 1
Firmware Version       : 1.00.001
Device Name            :
MAC Address             : F0-7D-00-36-30-B0
Platform               : DGS-3130-30TS
Hold Time              : 100 sec

Switch#
```

В данном примере показано, как отобразить список Candidate Switch SIM-группы.

```
Switch#show sim candidates

Candidate
  ID      MAC Address      Platform      Hold Time  Firmware Version  Device Name
-----
  1       EE-FF-00-00-12-12  DGS-3130-30TS  90        1.00.001
-----

Total Entries : 1

Switch#
```

В данном примере показано, как отобразить подробную информацию об одном определенном Candidate Switch SIM-группы.

```
Switch# show sim candidates 1

Sim Candidate Information :
Candidate ID      : 1
Firmware Version : 1.00.001
Device Name      :
MAC Address      : EE-FF-00-00-12-12
Platform         : DGS-3130-30TS
Hold Time        : 100 sec

Switch#
```

В данном примере показано, как отобразить краткую информацию о группе.

```
Switch# show sim group
* -means Commander switch.

SIM Group Name : default

ID  MAC Address      Platform      Hold Time  Firmware Version  Device Name
-----
*1  00-02-00-00-08-12  DGS-3130-30TS  40        1.00.001
  2  00-07-15-34-00-50
  3  00-01-02-03-00-10

SIM Group Name : SIM2

ID  MAC Address      Platform      Hold Time  Firmware Version  Device Name
-----
*1  00-01-02-03-04-11  DGS-3130-30TS  40        1.00.001
  2  00-55-55-00-55-11

Total Entries : 2

Switch#
```

В данном примере показано, как отобразить подробную информацию о группе.

```
Switch# show sim group 00-02-00-00-08-12

Sim Group Information :

[*** Commander Info ***]

MAC Address : 00-02-00-00-08-12
Group Name  : default
Device Name :
Firmware Version : 1.00.001
Platform    : DGS-3130-30TS
Number of Members : 2
Hold Time   : 100 sec

[*** Member Info (1/2)***]
MAC Address : 00-07-15-34-00-50

[*** Member Info (2/2)***]
MAC Address : 00-01-02-03-00-10

Switch#
```

В данном примере показано, как отобразить краткую информацию о соседних устройствах SIM- группы.

```
Switch# show sim neighbor

Port  MAC Address      Role
-----
1     00-02-00-00-08-12 Member
2     00-01-00-00-12-12 Member
2     EE-FF-00-00-12-12 Candidate

Total Entries : 3

Switch#
```


84. Команды Spanning Tree Protocol (STP)

84-1 clear spanning-tree detected-protocols

Данная команда используется для перезапуска процесса миграции протокола.

```
clear spanning-tree detected-protocols {all | interface INTERFACE-ID}
```

Параметры

all	Укажите, чтобы запустить действие обнаружения для всех портов.
<i>INTERFACE-ID</i>	Укажите интерфейс порта, на котором необходимо запустить действие обнаружения.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

С помощью данной команды во время миграции протокола порт будет переведен в состояние *SEND_RSTP*. Данное действие можно использовать, чтобы проверить, все ли устаревшие мосты на LAN были удалены. При отсутствии моста STP на данной LAN порт будет работать в выбранном режиме RSTP или MSTP. В противном случае порт будет работать в режиме STP.

Пример

В данном примере показано, как запустить процесс миграции протокола для всех портов.

```
Switch# clear spanning-tree detected-protocols all
Clear spanning-tree detected-protocols? (y/n) [n] y
Switch#
```

84-2 show spanning-tree

Данная команда используется для отображения информации о работе протокола Spanning Tree и применяется только для STP и RSTP.

```
show spanning-tree [interface [INTERFACE-ID [, | -]]]
```

Параметры

interface <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

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду для отображения настроек Spanning Tree одного связующего дерева в режиме, совместимом с RSTP или STP.

Пример

В данном примере показано, как отобразить информацию о Spanning Tree при включенном STP.

```
Switch#show spanning-tree

Spanning Tree: Enabled
Protocol Mode: RSTP
Tx-hold-count: 6
NNI BPDU Address: dot1d(01-80-C2-00-00-00)
Root ID Priority: 32768
    Address: F0-7D-68-34-0A-00
    Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
Bridge ID Priority: 32768 (priority 32768 sys-id-ext 0)
    Address: F0-7D-68-34-0A-00
    Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec,
Topology Changes Count: 0

Interface      Role      State      Cost      Priority Link
-----      -
eth1/0/1      designated forwarding 200000    128.1    p2p    edge

Switch#
```

84-3 show spanning-tree mst

Данная команда используется для отображения информации о Multiple Spanning Tree (MST) и его экземплярах (Instances).

show spanning-tree mst {configuration | instance *INSTANCE-ID* [interface *INTERFACE-ID*]}

Параметры

configuration	Укажите настройки MST оборудования.
instance <i>INSTANCE-ID</i>	Укажите номер экземпляра.
interface <i>INTERFACE-ID</i>	Укажите ID интерфейса, который необходимо отобразить.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию об MST.

Пример

В данном примере показано, как отобразить информацию о настройках Spanning Tree для Ethernet 1/0/1.

```
Switch#show spanning-tree mst configuration

Name      : F0:7D:68:34:00:10
Revision  : 0, Instances configured: 1
Instance  Vians
-----  -----
      0    1-4094

Switch#
```

84-4 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

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду для отображения настроек интерфейса Spanning Tree. Команда может быть использована для всех версий STP.

Пример

В данном примере показано, как отобразить информацию о настройках Spanning Tree для интерфейса Ethernet 1/0/1.

```
Switch#show spanning-tree configuration interface ethernet 1/0/1

eth1/0/1
Spanning tree state : Enabled
Port path cost: 0
Port priority: 128
Port Identifier: 128.1
Link type: auto
Port fast: edge
Guard root: Disabled
TCN filter : Disabled
Bpdu forward: Disabled

Switch#
```

84-5 snmp-server enable traps stp

Данная команда используется для включения отправки SNMP-уведомлений для STP. Используйте форму **no**, чтобы отключить отставку уведомлений для STP.

```
snmp-server enable traps stp [new-root] [topology-chg]
no snmp-server enable traps stp [new-root] [topology-chg]
```

Параметры

new-root	(Опционально) Укажите для отправки уведомлений о новом корне STP.
topology-chg	(Опционально) Укажите для отправки уведомлений об изменении STP- топологии.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить/отключить отправку trap-уведомлений. Если ни один из опциональных параметров не указан в форме **no** данной команды, будут отключены оба типа уведомлений STP.

Пример

В данном примере показано, как включить отправку всех STP trap на узел 10.9.18.100, используя строку сообщества «public».

```
Switch# configure terminal
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server enable traps stp
Switch(config)# snmp-server host 10.9.18.100 version 2c public
Switch(config)#
```

84-6 spanning-tree mst configuration

Данная команда используется для входа в режим MST Configuration и настройки MSTP-региона. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

spanning-tree mst configuration
no spanning-tree mst configuration

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы войти 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)#
```

84-7 instance

Данная команда используется для привязки VLAN к MST-экземпляру. Используйте команду **no instance** *INSTANCE-ID*, чтобы удалить указанный MST-экземпляр. Используйте команду **no instance** *INSTANCE-ID vlans VLAN-ID* [, | -], чтобы вернуть привязку VLAN к экземпляру по умолчанию (CIST).

```
instance INSTANCE-ID vlans VLAN-ID [, | -]
no instance INSTANCE-ID [vlans VLAN-ID [, | -]]
```

Параметры

<i>INSTANCE-ID</i>	Укажите ID MSTP-экземпляра, к которому необходимо привязать указанные VLAN. Доступный диапазон значений: от 1 до 64.
<i>VLAN-ID</i>	Укажите ID VLAN, который необходимо настроить.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию все VLAN привязаны к CIST, значение экземпляра которого 0.

Режим ввода команды

MST Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы привязать VLAN к MST-экземпляру. Во время привязки VLAN к несуществующему MST-экземпляру, MST-экземпляр будет создан автоматически.

Пример

В данном примере показано, как привязать несколько VLAN к MST-экземпляру.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance 2 vlans 1-100
Switch(config-mst)#
```

84-8 name

Данная команда используется для настройки имени MST-региона. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

name *NAME*
no name

Параметры

<i>NAME</i>	Укажите имя MST-региона. Максимально допустимое количество символов – 32.
-------------	---

По умолчанию

Имя по умолчанию – MAC-адрес моста.

Режим ввода команды

MST Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить имя MST-региона. 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 MST-региона. Настроенное имя – MSTP.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#name MSTP
Switch(config-mst)#
```

84-9 revision

Данная команда используется для настройки номера ревизии для MST. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

revision *REVISION*
no revision

Параметры

<i>REVISION</i>	При совпадении имен укажите другой уровень ревизии. Доступный диапазон значений: от 0 до 65535.
-----------------	--

По умолчанию

Значение по умолчанию – 0.

Режим ввода команды

MST Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить номер ревизии для MST. Коммутаторы с идентичной конфигурацией принадлежат к разным MST-регионам, если их номера ревизии не совпадают.

Пример

В данном примере показано, как настроить номер ревизии MST. Настроенное значение – 2.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#revision 2
Switch(config-mst)#
```

84- 10 spanning-tree mst

Данная команда используется для настройки стоимости пути и приоритета порта для MST- экземпляра. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

spanning-tree mst *INSTANCE-ID* {**cost** *COST* | **port-priority** *PRIORITY*}
no spanning-tree mst *INSTANCE-ID* {**cost** | **port-priority**}

Параметры

<i>INSTANCE-ID</i>	Укажите ID MSTP-экземпляра. Доступный диапазон значений: от 0 до 64. Значение экземпляра по умолчанию, CIST – 0.
cost <i>COST</i>	Укажите стоимость пути экземпляра. Доступный диапазон значений: от 0 до 200000000.

port-priority <i>PRIORITY</i>	Укажите приоритет порта экземпляра. Доступный диапазон значений: от 0 до 240 с шагом 16.
--------------------------------------	--

По умолчанию

Стоимость определяется на основе скорости порта. Чем выше скорость, тем меньше стоимость. MST всегда использует стоимость длинного пути.

Приоритет порта по умолчанию – 128.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется только для физических портов.

Пример

В данном примере показано, как настроить стоимость пути интерфейса.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/3
Switch(config-if)#spanning-tree mst 0 cost 17031970
Switch(config-if)#
```

В данном примере показано, как настроить приоритет порта.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/3
Switch(config-if)#spanning-tree mst 0 port-priority 64
Switch(config-if)#
```

84- 11 spanning-tree mst max-hops

Данная команда используется для настройки максимального числа переходов MSTP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
spanning-tree mst max-hops HOP-COUNT
no spanning-tree mst max-hops
```

Параметры

<i>HOP-COUNT</i>	Укажите максимальное число переходов MSTP. Доступный диапазон значений: от 1 до 40.
------------------	---

По умолчанию

Максимальное число переходов MSTP по умолчанию – 20.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить максимальное число переходов MSTP.

Пример

В данном примере показано, как настроить максимальное число переходов MSTP.

```
Switch#configure terminal
Switch(config)#spanning-tree mst max-hops 19
Switch(config)#
```

84-12 spanning-tree global state

Данная команда используется для включения/отключения глобального состояния STP. Используйте форму **no**, чтобы отключить глобальное состояние STP.

spanning-tree global state {enable | disable}
no spanning-tree global state

Параметры

enable	Укажите, чтобы включить глобальное состояние STP.
disable	Укажите, чтобы отключить глобальное состояние STP.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду в режиме Global Configuration Mode, чтобы включить функцию Spanning Tree глобально.

Пример

В данном примере показано, как включить функцию Spanning Tree.

```
Switch# configure terminal
Switch(config)# spanning-tree global state enable
Switch(config)#
```

84-13 spanning-tree (timers)

Данная команда используется для настройки значений таймеров Spanning Tree. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
spanning-tree {hello-time SECONDS | forward-time SECONDS | max-age SECONDS}
no spanning-tree {hello-time | forward-time | max-age}
```

Параметры

hello-time SECONDS	Укажите интервал между циклической передачей конфигурационных сообщений. Доступный диапазон значений: от 1 до 2 секунд.
forward-time SECONDS	Укажите время задержки продвижения (Forward Delay), используемое STP для перехода из состояния Listening и Learning в состояние Forwarding. Доступный диапазон значений: от 4 до 30 секунд.
max-age SECONDS	Укажите максимальное время жизни сообщения BPDU. Доступный диапазон значений: от 4 до 30 секунд.

По умолчанию

Значение параметра **hello-time** по умолчанию – 2 секунды.
 Значение параметра **forward-time** по умолчанию – 15 секунд.
 Значение параметра **max-age** по умолчанию – 20 секунд.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить значения таймеров Spanning Tree.

Пример

В данном примере показано, как настроить значения таймеров Spanning Tree.

```
Switch# configure terminal
Switch(config)# spanning-tree hello-time 1
Switch(config)# spanning-tree forward-time 16
Switch(config)# spanning-tree max-age 21
Switch(config)#
```

84- 14 spanning-tree state

Данная команда используется для включения /отключения STP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

spanning-tree state {enable | disable}
no spanning-tree state

Параметры

enable	Укажите, чтобы включить STP для настраиваемого интерфейса.
disable	Укажите, чтобы отключить STP для настраиваемого интерфейса.

По умолчанию

По умолчанию функция включена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если Spanning Tree включено, BPDU, полученный портом, будет либо отправлен, либо обработан. Используя данную команду, не допускайте появления петель. Данная команда не будет применена, если функция L2PT включена для STP.

Пример

В данном примере показано, как включить Spanning Tree на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# spanning-tree state enable
Switch(config-if)#
```

84- 15 spanning-tree cost

Данная команда используется для настройки значения стоимости пути на указанном порту. Используйте форму **no**, чтобы определить стоимость пути автоматически.

spanning-tree cost COST
no spanning-tree cost

Параметры

COST	Укажите стоимость пути для порта. Доступный диапазон
-------------	--

значений: от 1 до 200000000.

По умолчанию

По умолчанию стоимость пути определяется на основе настроек полосы пропускания интерфейса.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

В режимах, совместимых с STP и RSTP, для одного связующего дерева стоимость пути, заданная администратором, используется для достижения корня (Root). В режиме MSTP региональным корнем CIST (CIST Regional Root) используется стоимость пути, заданная администратором, для достижения корня CIST (CIST Root).

Пример

В данном примере показано, как настроить значение стоимости пути на интерфейсе Ethernet 1/0/7. Настроенное значение: 20000.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/7
Switch(config-if)# spanning-tree cost 20000
Switch(config-if)#
```

84-16 spanning-tree mst hello-time

Данная команда используется для настройки параметра Hello Time в версии MSTP для каждого порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

spanning-tree mst hello-time SECONDS
no spanning-tree mst hello-time

Параметры

<i>SECONDS</i>	Укажите интервал между отправкой одного BDPU-сообщения для назначенного порта (Designated Port). Доступный диапазон значений: от 1 до 2 секунд.
----------------	---

По умолчанию

Значение параметра Hello Time по умолчанию – 2 секунды.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки параметра Hello Time в версии MSTP для каждого порта. 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.

```
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#spanning-tree mst hello-time 1
Switch(config-if)#
```

84- 17 spanning-tree loop-guard

Данная команда используется для включения функции Loop Guard. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
spanning-tree loop-guard
no spanning-tree loop-guard
```

Параметры

Нет

По умолчанию

По умолчанию функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для интерфейсов порта и port-channel.

Функция STP Loop Guard обеспечивает дополнительную защиту от петель в L2 домене (петель STP). Петля STP образуется, когда заблокированный порт в резервной топологии ошибочно переходит в состояние Forwarding, по причине того, что один из портов (не обязательно заблокированный порт) перестает получать пакеты BPDU протокола STP, работа которого зависит от непрерывного получения и передачи BPDU на основе роли порта. Назначенный порт (Designated Port) передает BPDU, а не назначенный порт (Non-designated Port) получает BPDU.

Когда один из портов в физически резервной топологии перестает получать BPDU, протокол STP определяет, что в данной топологии отсутствуют петли. В итоге роль заблокированного порта изменяется с

альтернативного/резервного порта (Alternate/Backup Port) на назначенный (Designated) порт, который переходит в состояние Forwarding. В данной ситуации образуется петля.

Пример

В данном примере показано, как включить функцию Loop Guard на интерфейсе Ethernet 1/0/3.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/3
Switch(config-if)#spanning-tree loop-guard
Switch(config-if)#
```

84-18 spanning-tree guard root

Данная команда используется для включения функции STP Root Guard. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

spanning-tree guard root
no spanning-tree guard root

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

BPDU Guard предотвращает превращение порта в корневой порт и ограничивает доступ внешним мостам, находящимся не под полным контролем администратора, к основному региону сети активной топологии связующего дерева.

Порт, которому было отказано в присвоении роли корневого порта (Root Port), сможет работать только в качестве назначенного порта (Designated Port). При получении конфигурационного BPDU с более высоким приоритетом порт начнет работать в качестве альтернативного порта (Alternate Port) в состоянии «Blocking». Получение BPDU с более высоким приоритетом не повлияет на построение STP. Порт будет прослушивать сообщения BPDU. Если время ожидания получения BPDU с наибольшим приоритетом истечет, порт начнет работать в качестве назначенного порта.

Когда функция Guard Root сработает и порт начнет работать в качестве альтернативного порта, будет сгенерировано системное сообщение. Данные настройки действительны для всех версий Spanning Tree.

Пример

В данном примере показано, как предотвратить смену роли порта на роль корневого порта (Root port) для интерфейса Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# spanning-tree guard root
Switch(config-if)#
```

84-19 spanning-tree link-type

Данная команда используется для настройки типа соединения (Link-type) для порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

spanning-tree link-type {point-to-point | shared}
no spanning-tree link-type

Параметры

point-to-point	Укажите тип соединения «точка-точка» (Point To Point, P2P).
shared	Укажите тип соединения для подключения к сети общего пользования (Shared Media).

По умолчанию

Если ни один из параметров не указан, тип соединения по умолчанию назначается на основе настроек дуплекса.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

На портах, функционирующих в режиме полного дуплекса, устанавливается соединение Point To Point; порты, работающие в режиме полудуплекса, считаются портами общего пользования (Shared Port). Так как быстрый переход в состояние Forwarding при использовании типа соединения Shared Media невозможен, рекомендуется использовать автоматическое определение Link-type модулем STP.

Данные настройки действительны для всех режимов Spanning Tree.

Пример

В данном примере показано, как настроить тип соединения Point To Point для Ethernet-порта 1/0/7.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/7
Switch(config-if)# spanning-tree link-type point-to-point
Switch(config-if)#
```


84-20 spanning-tree mode

Данная команда используется для настройки режима STP. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
spanning-tree mode {mstp | rstp | stp}
no spanning-tree mode
```

Параметры

mstp	Укажите Multiple Spanning Tree Protocol (MSTP).
rstp	Укажите Rapid Spanning Tree Protocol (RSTP).
stp	Укажите Spanning Tree Protocol (совместимый с IEEE 802.1D).

По умолчанию

Режим по умолчанию – RSTP.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если настраивается режим STP или RSTP, все текущие MSTP-экземпляры будут отменены автоматически. При изменении режима Spanning Tree все порты перейдут в состояние Discarding (отбрасывание).

Пример

В данном примере показано, как настроить текущую версию протокола STP на RSTP.

```
Switch# configure terminal
Switch(config)# spanning-tree mode rstp
Switch(config)#
```

84-21 spanning-tree portfast

Данная команда используется для настройки режима Port Fast на порту. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
spanning-tree portfast {disable | edge| network}
no spanning-tree portfast
```

Параметры

disable	Укажите для включения режима Fast Disable на порту.
edge	Укажите для включения режима Fast Edge на порту.
network	Укажите для включения режима Fast Network на порту.

По умолчанию

Режим по умолчанию – Edge Mode.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

На порту может быть установлен один из трех режимов Port Fast:

- **Edge Mode:** при установлении соединения порт сразу же переходит в состояние Forwarding, не дожидаясь задержки продвижения (Forward Delay). Рабочее состояние интерфейса, на котором BPDU было получено позже, будет изменено на состояние Non-Port-Fast.
- **Disable Mode:** порт всегда находится в состоянии Non-Port-Fast и будет ждать, пока Forward Delay не перейдет в состояние Forwarding.
- **Network Mode:** порт находится в состоянии Non-Port-Fast в течение трех секунд. Не получив BPDU, порт переходит в состояние Port-Fast, за которым следует состояние Forwarding. Состояние порта, на котором BPDU было получено позже, будет изменено на состояние Non-Port-Fast.

Применяя данную команду, не допускайте появления петель в топологии и петель во время передачи пакетов данных, которые нарушают работу сети.

Пример

В данном примере показано, как настроить режим Port-Fast Edge для Ethernet-порта 1/0/7.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/7
Switch(config-if)# spanning-tree portfast edge
Switch(config-if)#
```

84-22 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

<i>PRIORITY</i>	Укажите приоритет порта в диапазоне от 0 до 240.
-----------------	--

По умолчанию

Значение по умолчанию – 128.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

При присвоении роли порту используется его идентификатор, который состоит из приоритета и номера порта. Чем ниже число, тем выше приоритет. Данный параметр применим только в режимах RSTP или STP.

Пример

В данном примере показано, как настроить приоритет для Ethernet-порта 1/0/7 со значением 0.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/7
Switch(config-if)# spanning-tree port-priority 0
Switch(config-if)#
```

84-23 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Выбор корневого моста зависит от значения приоритета моста и системного MAC-адреса. Значение приоритета моста должно делиться на 4096. Чем меньше число, тем выше приоритет.

Данные настройки применимы для версий STP и RSTP протокола Spanning Tree. В режиме MSTP используйте команду **spanning-tree mst priority**, чтобы настроить приоритет для MSTP-экземпляра.

Пример

В данном примере показано, как настроить приоритет моста STP со значением 4096.

```
Switch# configure terminal
Switch(config)# spanning-tree priority 4096
Switch(config)#
```

84-24 spanning-tree tcnfilter

Данная команда используется для включения фильтрации уведомлений об изменении топологии сети TCN (Topology Change Notification) на указанном интерфейсе. Используйте форму **no**, чтобы отключить фильтрацию TCN.

spanning-tree tcnfilter
no spanning-tree tcnfilter

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Фильтрация TCN используется для защиты ISP от подключения внешних мостов, находящихся не под полным контролем администратора, к основному региону сети, в котором в данной ситуации произойдет очистка (Flush) адресов.

В режиме фильтрации уведомление TCN об изменении топологии, полученное на порту, игнорируется. Данные настройки действительны для всех режимов Spanning Tree.

Пример

В данном примере показано, как включить фильтрацию TCN на Ethernet-порту 1/0/7.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/7
Switch(config-if)# spanning-tree tcnfilter
Switch(config-if)#
```

84-25 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать максимальное количество отправляемых BPDU. Передача BPDU на порт контролируется счетчиком, значение которого увеличивается при каждой отправке BPDU и уменьшается раз в секунду. Передача BPDU приостанавливается на одну секунду, если счетчик достигает значения параметра Hold Count.

Пример

В данном примере показано, как настроить параметр Hold Count со значением 5.

```
Switch# configure terminal
Switch(config)# spanning-tree tx-hold-count 5
Switch(config)#
```

84-26 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

Уровень команды по умолчанию

Уровень 12

Использование команды

При использовании данной команды полученные STP BPDU будут перенаправлены на все Member-порты VLAN без тега. Данная команда не будет применена, если функция L2PT включена для STP.

Пример

В данном примере показано, как включить 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)#
```

84-27 spanning-tree nni-bpdu-address

Данная команда используется для для настройки адреса назначения STP BPDU на стороне провайдера. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
spanning-tree nni-bpdu-address {dot1d | dot1ad}
no spanning-tree nni-bpdu-address
```

Параметры

dot1d	Укажите Customer Bridge Group Address (01-80-C2-00-00-00) в качестве адреса назначения STP BPDU.
dot1ad	Укажите Provider Bridge Group Address (01-80-C2-00-00-00) в качестве адреса назначения STP BPDU.

По умолчанию

По умолчанию в качестве адреса назначения STP BPDU используется пользовательский адрес группы моста (Customer Bridge Group Address).

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Как правило, в качестве адреса назначения STP BPDU используется пользовательский адрес группы моста (Customer Bridge Group Address). Данная команда используется для указания адреса назначения STP BPDU на стороне провайдера и применима только на trunk-портах VLAN, которые выступают в роли NNI-портов на стороне провайдера.

Данные настройки действительны для всех режимов Spanning Tree.

Пример

В данном примере показано, как указать адрес «**dot1ad**» в качестве адреса назначения BPDU на trunk-порту VLAN.

```
Switch# configure terminal
Switch(config)# spanning-tree nni-bpdu-address dot1ad
Switch(config)#
```

85. Команды стекирования

85-1 stack

Данная команда используется для включения функции линейного стекирования. Используйте форму **no**, чтобы отключить функцию линейного стекирования.

stack
no stack

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Порты, используемые для подключения к другим коммутаторам, могут работать как порты стекирования или как обычные Ethernet-порты в зависимости от настройки команды стека. Настройки данной команды необходимо применить перед стекированием коммутаторов. При необходимости настройки могут быть сохранены в отдельном Unit.

При стекировании последние 2 или 4 порта SFP+ предназначены только для стекирования и не могут быть использованы для каких-либо других целей. Данные порты могут быть использованы для стекирования, только если данная функция включена.

Пример

В данном примере показано, как включить режим стекирования.

```
Switch#stack  
  
WARNING: The command does not take effect until the next reboot.  
Switch#
```

85-2 stack bandwidth

Данная команда используется для изменения пропускной способности порта стекирования. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

stack bandwidth {2-port | 4-port}

no stack bandwidth**Параметры**

2-port	Укажите, чтобы использовать для стекирования 2 порта.
4-port	Укажите, чтобы использовать для стекирования 4 порта.

По умолчанию

По умолчанию используются 2 порта.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для изменения пропускной способности порта стекирования. Пропускную способность необходимо настроить перед стекированием коммутаторов.

Необходимо включить физическое стекирование и при необходимости указать в настройках количество портов (2 или 4), которые будут использованы для стекирования.

Если для стекирования используется два порта, между двумя коммутаторами будет установлено соединение на скорости до 40 Гбит/с в режиме полного дуплекса. Ниже перечислены порты, которые могут быть использованы для данного типа стекирования.

- Коммутаторы ТГК-313-24Х: физические порты 25 (SIO1) и 26 (SIO2).
- Коммутаторы ТГК-313-24Х: физические порты 29 (SIO1) и 30 (SIO2).
- Коммутаторы ТГК-313-48Х: физические порты 49 (SIO1) и 50 (SIO2).
- Коммутаторы ТГК-313-48Х: физические порты 53 (SIO1) и 54 (SIO2).

Если для стекирования используется четыре порта, между двумя коммутаторами будет установлено соединение на скорости до 80 Гбит/с в режиме полного дуплекса, при этом четыре физических порта будут объединены в два виртуальных порта стекирования. Ниже перечислены порты, которые могут быть использованы для данного типа стекирования.

- Коммутаторы ТГК-313-24Х: физические порты 25 (SIO1), 26 (SIO2), 29 (SIO1) и 30 (SIO2).
- Коммутаторы ТГК-313-24Х: физические порты 27 (SIO1), 28 (SIO2), 29 (SIO1) и 30 (SIO2).
- Коммутаторы ТГК-313-48Х: физические порты 49 (SIO1), 50 (SIO2), 53 (SIO1) и 54 (SIO2).
- Коммутаторы ТГК-313-48Х: физические порты 51 (SIO1), 52 (SIO2), 53 (SIO1) и 54 (SIO2).

Порты стекирования SIO1 и SIO2 являются логической парой, которая должна быть подключена к одному и тому же коммутатору в стеке. Если порты данной пары подключены к разным коммутаторам, стабильное подключение при стекировании не гарантировано.

Пример

В данном примере показано, как изменить пропускную способность и использовать для стекирования 4 порта.

```
Switch#stack bandwidth 4-port

WARNING: The command does not take effect until the next reboot.
Switch#
```

85-3 stack renumber

Данная команда используется для назначения Unit ID коммутатору вручную. Используйте форму **no**, чтобы назначить Unit ID коммутатору автоматически.

```
stack CURRENT-UNIT-ID renumber NEW-UNIT-ID
no stack CURRENT-UNIT-ID renumber
```

Параметры

<i>CURRENT-UNIT-ID</i>	Укажите текущий Unit ID коммутатора.
<i>NEW-UNIT-ID</i>	Укажите новый Unit ID, который необходимо назначить коммутатору.

По умолчанию

По умолчанию Unit ID назначается автоматически.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Изначально у коммутатора отсутствует Unit ID. При инициализации или добавлении в стек коммутатора Unit ID будет автоматически назначен основным устройством (Master). Unit ID можно сохранить в конфигурационном файле после его назначения, применив команду **copy running-config startup-config**. Сохранившийся Unit ID будет использован при следующем запуске устройства.

Используйте данную команду для переназначения Unit ID указанного коммутатора. Назначенный Unit ID будет использован при следующем запуске устройства.

При автоматическом назначении Unit ID основным устройством (Master) применяются следующие правила:

- Unit ID основного устройства (Master) при автоматическом назначении – 1.
- Коммутатор не будет добавлен в стек при обнаружении конфликта его Unit ID с существующим Unit ID.

Пример

В данном примере показано, как изменить Unit ID коммутатора. Прежний ID – 2. Новый ID – 3.

```
Switch# stack 2 renumber 3
WARNING: The command does not take effect until the next reboot.
Switch#
```

85-4 stack priority

Данная команда используется для настройки приоритета коммутатора в стеке. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
stack CURRENT-UNIT-ID priority NEW-PRIORITY-NUMBER
no stack CURRENT-UNIT-ID priority
```

Параметры

<i>CURRENT-UNIT-ID</i>	Укажите текущий Unit ID коммутатора.
<i>NEW-PRIORITY-NUMBER</i>	Укажите приоритет, который необходимо назначить Unit коммутатора в стеке. Доступный диапазон значений: от 1 до 63. Чем меньше номер, тем выше приоритет.

По умолчанию

Значение по умолчанию – 32.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для настройки приоритета указанного коммутатора. Среди коммутаторов, объединенных в стек линейной топологии, основным устройством (Master) становится коммутатор с наивысшим приоритетом. Следующий по приоритету коммутатор будет выбран в качестве резервного устройства (Backup master). Чем меньше значение, тем выше приоритет. Если приоритеты коммутаторов равны, высший приоритет получает коммутатор с наименьшим значением MAC-адреса. При необходимости настройки могут быть сохранены в отдельном Unit.

Пример

В данном примере показано, как настроить приоритет Unit 2 коммутатора со значением 10.

```
Switch# stack 2 priority 10
Switch#
```

85-5 stack preempt

Данная команда используется для включения функции Preempt, с помощью которой можно присвоить роль основного устройства (Master) коммутатору, который будет добавлен в стек, если его приоритет выше, чем у текущего основного устройства. Используйте форму **no**, чтобы отключить функцию Preempt.

stack preempt
no stack preempt

Параметры

Нет

По умолчанию

По умолчанию функция включена.

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если функция Preempt отключена, роль основного устройства (Master) не будет присвоена коммутатору, который будет добавлен в стек, даже если его приоритет выше, чем у текущего основного устройства. Если функция Preempt включена, то роль основного устройства (Master) будет присвоена коммутатору, который будет добавлен в стек, если его приоритет выше, чем у текущего основного устройства.

Пример

В данном примере показано, как включить функцию Preempt.

```
Switch# stack preepmt  
Switch#
```

85-6 snmp-server enable traps stack

Данная команда используется для включения отправки trap-сообщений, касающихся стекирования. Используйте форму **no**, чтобы отключить отpravку trap-сообщений, касающихся стекирования.

snmp-server enable traps stack
no snmp-server enable traps stack

Параметры

Нет

По умолчанию

По умолчанию функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить/отключить отправку SNMP-уведомлений, касающихся стекирования.

Пример

В данном примере показано, как включить отправку trap-сообщений, касающихся стекирования.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps stack
Switch(config)#
```

85-7 show stack

Данная команда используется для отображения информации о стекировании.

show stack

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить информацию о стекировании.

Пример

В данном примере показано, как отобразить информацию о стекировании.

```
Switch#show stack

Stacking Mode      : Enabled
Stack Preempt     : Enabled
Trap State        : Disabled

Topology          : Duplex_Chain
My Box ID         : 1
Master ID         : 1
Box Count         : 1

Box User Module      Prio-      Prom      Runtime  H/W
ID Set  Name          Exist rity MAC      Version   Version   Version
-----
1  Auto DGS-3130-30TS Exist 32   F0-7D-68-36-30-B0 1.00.001  1.00.001  A1
2  -    NOT_EXIST     No
3  -    NOT_EXIST     No
4  -    NOT_EXIST     No
5  -    NOT_EXIST     No
6  -    NOT_EXIST     No
7  -    NOT_EXIST     No
8  -    NOT_EXIST     No
9  -    NOT_EXIST     No

Stack Bandwidth:
Box  User Set  SIO1 Active  SIO2 Active
ID   Bandwidth  Bandwidth    Bandwidth
----
1    2-port    Down         Down
2
3
4
5
6
7
8
9

Switch#
```

86. Команды Storm Control

86-1 snmp-server enable traps storm-control

Данная команда используется для включения и настройки отправки SNMP-уведомлений для Storm Control. Используйте форму **no**, чтобы отключить отправку SNMP-уведомлений.

```
snmp-server enable traps storm-control [storm-occur] [storm-clear]
no snmp-server enable traps storm-control [storm-occur] [storm-clear]
```

Параметры

storm-occur	(Опционально) Укажите для отправки уведомлений при возникновении шторма.
storm-clear	(Опционально) Укажите для отправки уведомлений при предотвращении шторма.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения и настройки отправки SNMP-уведомлений для Storm Control.

Пример

В данном примере показано, как включить отправку trap-сообщений при возникновении и предотвращении шторма.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps storm-control
Switch(config)#
```

86-2 storm-control

Данная команда используется для защиты устройства от штормовых атак широковещательных и многоадресных пакетов или пакетов с неизвестным адресом назначения. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
storm-control {{broadcast | multicast | unicast} level {pps PPS-RISE [PPS-LOW] | kbps KBPS-RISE
[KBPS-LOW] | LEVEL-RISE [LEVEL-LOW]} | action {shutdown | drop | none}}
no storm-control {broadcast | multicast | unicast | action}
```

Параметры

broadcast	Укажите для ограничения скорости широковещательной рассылки.
multicast	Укажите для ограничения скорости многоадресной рассылки.
unicast	Укажите, чтобы в режиме shutdown применять команду как к известным, так и к неизвестным одноадресным пакетам. При достижении на порту установленного лимита пакетов порт будет отключен. Если указан другой режим, команда будет применена только к неизвестным одноадресным пакетам.
level pps <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.
level kbps <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.
level <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).
action shutdown	Укажите, чтобы отключить порт при достижении указанного максимального порогового значения.
action drop	Укажите, чтобы отбросить пакеты, которые превышают максимальный порог.
action none	Укажите, чтобы не фильтровать Storm пакеты.

По умолчанию

Storm Control широковещательной, многоадресной и одноадресной (DLF) рассылки по умолчанию отключен.

При возникновении шторма по умолчанию Storm пакеты будут отброшены.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Функция Storm Control используется для защиты сети от штормовых атак широковещательных и многоадресных пакетов или пакетов с неизвестным адресом назначения лавинной рассылки.

Используйте команду **storm-control**, чтобы включить Storm Control для определенного типа трафика на интерфейсе.

Пример

В данном примере показано, как включить Storm Control для управления широковещательным штормом на интерфейсах Ethernet 1/0/1 и Ethernet 1/0/2. На Ethernet 1/0/1 установлен порог до 500 пакетов в секунду с действием отключения (Shutdown). На интерфейсе порта 3,2 установлен порог до 70% с действием отбрасывания (Drop).

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# storm-control broadcast level pps 500
Switch(config-if)# storm-control action shutdown
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# storm-control broadcast level 70 60
Switch(config-if)# storm-control action drop
Switch(config-if)#
```

86-3 storm-control polling

Данная команда используется для настройки интервала опроса (Polling Interval) для подсчета количества полученных пакетов. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

storm-control polling {interval SECONDS | retries {NUMBER | infinite}}
no storm-control polling {interval | retries}

Параметры

interval SECONDS	Укажите интервал опроса для подсчета количества полученных пакетов. Доступный диапазон значений: от 1 до 300 секунд.
retries NUMBER	Укажите количество попыток интервалов между запросами. Если в режиме shutdown шторм продолжается во время установленных значений попыток, порт перейдет в состояние Error-Disabled. Доступный диапазон значений: от 0 до 360. 0 означает, что при обнаружении шторма порт в режиме shutdown сразу же будет отключен из-за ошибки. Infinite означает, что порт в режиме shutdown не будет отключен из-за ошибки даже при обнаружении шторма.

По умолчанию

Интервал опроса по умолчанию – 5 секунд.
 Количество попыток по умолчанию – 3.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать интервал выборки для подсчета количества полученных пакетов.

Пример

В данном примере показано, как указать интервал опроса на 15 секунд.

```
Switch# configure terminal
Switch(config)# storm-control polling interval 15
Switch(config)#
```

86-4 show storm-control

Данная команда используется для отображения текущих настроек функции Storm Control.

show storm-control interface *INTERFACE-ID* [, | -] [*broadcast* | *multicast* | *unicast*]

Параметры

interface <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.
broadcast	(Опционально) Укажите, чтобы отобразить текущие настройки шторма широкоэмитерных пакетов (Broadcast Storm).
multicast	(Опционально) Укажите, чтобы отобразить текущие настройки шторма многоадресных пакетов (Multicast Storm).
unicast	(Опционально) Укажите, чтобы отобразить текущие настройки шторма одноадресных пакетов (DLF).

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Если ID интерфейса не указан, будут отображены настройки всех интерфейсов. Если тип пакета не указан, будут отображены настройки всех типов Storm Control.

Пример

В данном примере показано, как отобразить текущие настройки Storm Control для широковещательных пакетов.

```
Switch# show storm-control interface ethernet 1/0/1-1/0/6 broadcast
```

Interface	Action	Threshold	Current	State
eth1/0/1	Drop	500/300 pps	200 pps	Forwarding
eth1/0/2	Drop	80/64 %	20 %	Forwarding
eth1/0/3	Drop	80/64 %	70 %	Dropped
eth1/0/4	Shutdown	60/50 %	20 %	Forwarding
eth1/0/5	None	60000/50000 kbps	2000 kbps	Forwarding
eth1/0/6	None	-	-	Inactive

```
Total Entries: 6
Switch#
```

В данном примере показано, как отобразить все настройки для диапазона интерфейсов от 3/0/1 до 3/0/2.

```
Switch# show storm-control interface eth1/0/1-2
```

```

Polling Interval      : 15 sec           Shutdown Retries     : Infinite
Trap                  : Disabled

```

Interface	Storm	Action	Threshold	Current	State
eth1/0/1	Broadcast	Drop	80/64 %	50%	Forwarding
eth1/0/1	Multicast	Drop	80/64 %	50%	Forwarding
eth1/0/1	Unicast	Drop	80/64 %	50%	Forwarding
eth1/0/2	Broadcast	Shutdown	500/300 pps	-	Error Disabled
eth1/0/2	Multicast	Shutdown	500/300 pps	-	Error Disabled
eth1/0/2	Unicast	Shutdown	500/300 pps	-	Error Disabled

```
Total Entries: 6
Switch#
```

Отображаемые параметры

Interface	ID интерфейса.
Action	Настраиваемые действия. Возможны следующие действия: Drop (отбрасывание), Shutdown (отключение), None (без действия).

Threshold	Настраиваемое пороговое значение.
Current	Фактическая текущая скорость трафика, которая проходит через интерфейс, единицей которой могут быть проценты, кбит/с, PPS в зависимости от настроенного режима. Аппаратно скорость может быть подсчитана только в PPS, приблизительно равного значению в процентах и кбит/с.
State	Текущее состояние Storm Control на указанном интерфейсе для данного типа трафика. Возможны следующие состояния: Forwarding: шторма не обнаружено. Dropped: шторм обнаружен, и штормовой трафик, превышающий пороговое значение, отбрасывается. Error Disabled: порт отключен из-за шторма. Link Down: порт физически отключен. Inactive: Storm Control не включен для данного типа трафика.

87. Команды Super VLAN

87-1 supervlan

Данная команда используется для настройки VLAN в качестве Super VLAN. Используйте форму **no**, чтобы удалить назначение Super VLAN.

```
supervlan
no supervlan
```

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для указания VLAN в качестве Super VLAN. Super VLAN используются для объединения нескольких Sub-VLAN (широковещательных L2 доменов) в IP-подсети. В Super VLAN не могут быть добавлены физические порты. Super VLAN не может одновременно быть Sub-VLAN. После привязки IP-интерфейса к Super VLAN опция Proxy ARP будет автоматически включена на интерфейсе для связи между ее Sub-VLAN. Возможна настройка нескольких Super VLAN, каждая из которых может состоять из нескольких Sub-VLAN.

Private VLAN не может быть настроена в качестве Super VLAN, так как они являются взаимоисключающими.

На интерфейсе Super VLAN не поддерживаются протоколы маршрутизации 3 уровня, VRRP, протоколы многоадресной рассылки и протокол IPv6.

Пример

В данном примере показано, как настроить VLAN 10 в качестве Super VLAN.

```
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#supervlan

WARNING: Proxy ARP will be enabled automatically on this super VLAN.
Switch(config-vlan)#
```

87-2 subvlan

Данная команда используется для добавления одной или нескольких Sub-VLAN в Super VLAN. Используйте форму **no**, чтобы удалить Sub-VLAN.

```
subvlan VLAN-ID [, | -]
no subvlan [VLAN-ID [, | -]]
```

Параметры

VLAN-ID	Укажите VLAN ID в качестве Sub-VLAN. Доступный диапазон значений: от 1 до 4094.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Sub-VLAN – это широковещательный L2 домен. Данная команда используется для настройки одной или нескольких Sub-VLAN, которые принадлежат одной Super VLAN. Private VLAN и Super VLAN являются взаимоисключающими.

Пример

В данном примере показано, как настроить VLAN 5, 6 и 7 в качестве Sub-VLAN, принадлежащих Super VLAN 10.

```
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#supervlan

WARNING: Proxy ARP will be enabled automatically on this super VLAN.
Switch(config-vlan)#subvlan 5-7
Switch(config-vlan)#
```

87-3 subvlan-address-range

Данная команда используется для настройки диапазона IP-адресов Sub-VLAN. Используйте форму **no**, чтобы удалить диапазон IP-адресов Sub-VLAN.

subvlan-address-range *START-IP-ADDRESS END-IP-ADDRESS*
no subvlan-address-range [*START-IP-ADDRESS END-IP-ADDRESS*]

Параметры

<i>START-IP-ADDRESS</i>	Укажите начальный IP-адрес необходимой Sub-VLAN.
<i>END-IP-ADDRESS</i>	Укажите конечный IP-адрес необходимой Sub-VLAN.

По умолчанию

Нет

Режим ввода команды

VLAN Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применима только на Sub-VLAN и используется для настройки ее диапазона/диапазонов IP-адресов, что может сократить издержки, если на коммутаторе подключена опция Proxy ARP между Sub-VLAN. Некорректная настройка диапазонов IP-адресов может привести к ошибкам маршрутизации IP-трафика. У Sub-VLAN может быть один или более диапазонов IP-адресов. Настраиваемый диапазон IP-адресов не должен совпадать с существующими диапазонами адресов других Sub-VLAN и должен принадлежать подсети интерфейса Super VLAN. В пределах Sub-VLAN настраиваемый диапазон IP-адресов будет объединен с другим диапазоном/диапазонами при необходимости.

Пример

В данном примере показано, как настроить диапазон IP-адресов Sub-VLAN 5.

```
Switch# configure terminal
Switch(config)# vlan 5
Switch(config-vlan)# subvlan-address-range 192.168.10.1 192.168.10.50
Switch(config-vlan)#
```

87-4 show supervlan

Данная команда используется для отображения настроек Super VLAN и ее Sub-VLAN.

show supervlan [VLAN-ID [, | -]]

Параметры

VLAN-ID	(Опционально) Укажите ID Super VLAN, которую необходимо отобразить.
,	(Опционально) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду для отображения настроек Super VLAN и ее Sub-VLAN.

Пример

В данном примере показано, как отобразить настройки всех Super VLAN.

```
Switch#show supervlan

SuperVLAN ID  SubVLAN ID  SubVLAN Status  SubVLAN IP Address Range
-----
10            5           Active          192.168.10.1 - 192.168.10.50
              6           Inactive        192.168.10.51 - 192.168.10.60
              7           Inactive        192.168.10.61 - 192.168.10.70

Switch#
```

88. Команды Surveillance VLAN

88-1 surveillance vlan

Данная команда используется для глобального включения функции Surveillance VLAN и ее настройки. Используйте форму **no**, чтобы отключить функцию Surveillance VLAN.

```
surveillance vlan VLAN-ID
no surveillance vlan
```

Параметры

VLAN-ID	Укажите VLAN ID Surveillance VLAN в диапазоне от 2 до 4094.
---------	---

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для глобального включения функции Surveillance VLAN и ее настройки на коммутаторе. На коммутаторе может быть настроена только одна Surveillance VLAN.

Для включения функции Surveillance VLAN необходимо применить команду **surveillance vlan** в режиме Global Configuration Mode и команду **surveillance vlan enable** в режиме Interface Configuration Mode.

При включении на порту Surveillance VLAN порт будет автоматически распознан как нетегированный член Surveillance VLAN, полученные нетегированные пакеты Surveillance будут перенаправлены в Surveillance VLAN. При соответствии исходных MAC-адресов пакетов адресам уникального идентификатора организации (OUI), настроенным при помощи команды **surveillance vlan mac-address**, полученные пакеты распознаются как пакеты Surveillance.

VLAN необходимо создать перед ее назначением в качестве Surveillance VLAN. Настроенную Surveillance VLAN нельзя удалить с помощью команды **no vlan**.

Пример

В данном примере показано, как включить функцию Surveillance VLAN и настроить VLAN 1001 в качестве Surveillance VLAN.

```
Switch# configure terminal
Switch(config)# surveillance vlan 1001
Switch(config)#
```


88-2 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для настройки времени устаревания для устройства Surveillance и автоматически изученных Member-портов Surveillance VLAN.

Когда последнее устройство Surveillance, подключенное к порту, перестает отправлять трафик и MAC- адрес данного устройства устаревает, запускается таймер времени устаревания Surveillance VLAN. По истечении данного времени порт будет удален из Surveillance VLAN.

Если трафик Surveillance возобновляется в течение времени устаревания, таймер будет отменен.

Пример

В данном примере показано, как настроить время устаревания Surveillance VLAN на 30 минут.

```
Switch# configure terminal
Switch(config)#surveillance vlan aging 30
Switch(config)#
```

88-3 surveillance vlan enable

Данная команда используется для включения функции Surveillance VLAN на портах. Используйте форму **no**, чтобы отключить функцию Surveillance VLAN на портах.

```
surveillance vlan enable
no surveillance vlan enable
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда доступна для настройки интерфейсов физического порта и port-channel. Команда используется на портах доступа и гибридных портах.

Для включения функции Surveillance VLAN необходимо применить команду **surveillance vlan** в режиме Global Configuration Mode и команду **surveillance vlan enable** в режиме Interface Configuration Mode.

При включении на порту Surveillance VLAN порт будет автоматически распознан как нетегированный член Surveillance VLAN. Полученные нетегированные пакеты Surveillance будут перенаправлены в Surveillance VLAN. При соответствии исходных MAC-адресов пакетов адресам уникального идентификатора организации (OUI), настроенным при помощи команды **surveillance vlan mac-address**, полученные пакеты распознаются как пакеты Surveillance.

Пример

В данном примере показано, как включить функцию Surveillance VLAN на физическом порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#surveillance vlan enable
Switch(config-if)#
```

88-4 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.
component-type	(Опционально) Укажите устройство системы

	видеонаблюдения, которое может быть автоматически обнаружено при помощи Surveillance VLAN.
vms	(Опционально) Укажите сервер VMS (Video Management Server – сервер для управления системой видеонаблюдения).
vms-client	(Опционально) Укажите клиента VMS в системе видеонаблюдения.
video-encoder	(Опционально) Укажите видеокодер в системе видеонаблюдения.
network-storage	(Опционально) Укажите сетевое хранилище в системе видеонаблюдения.
other	(Опционально) Укажите другие устройства в системе видеонаблюдения (IP Surveillance Devices).
description TEXT	(Опционально) Укажите описание OUI. Максимально допустимое количество символов – 32.

По умолчанию

OUI Address	Mask	Component Type	Description
28-10-7B-00-00-00	FF-FF-FF-E0-00-00	T-KOM Device	IP Surveillance
Device 28-10-7B-20-00-00	FF-FF-FF-F0-00-00	T-KOM Device	IP Surveillance
Device B0-C5-54-00-00-00	FF-FF-FF-80-00-00	T-KOM Device	IP Surveillance
Device F0-7D-68-00-00-00	FF-FF-FF-F0-00-00	T-KOM Device	IP Surveillance Device



Примечание: **Component Type** – устройство, определяемое в Surveillance VLAN.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для добавления одного или нескольких OUI Surveillance VLAN. OUI используется для идентификации трафика видеонаблюдения с помощью функции Surveillance VLAN. Если MAC-адреса источника полученных пакетов соответствуют любому из шаблонов OUI, полученный пакет распознается как Surveillance.

OUI, полученный с устройства видеонаблюдения в Surveillance VLAN, не может совпадать с OUI по умолчанию.

OUI по умолчанию не может быть удален.

Пример

В данном примере показано, как добавить OUI для устройств Surveillance.

```
Switch# configure terminal
Switch(config)# surveillance vlan mac-address 00-01-02-03-00-00 FF-FF-FF-FF-00-00 component-
type vms description user1
Switch(config)#
```

88-5 surveillance vlan qos

Данная команда используется для настройки приоритета CoS для входящего трафика Surveillance VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
surveillance vlan qos COS-VALUE
no surveillance vlan qos
```

Параметры

<i>COS-VALUE</i>	Укажите приоритет Surveillance VLAN в диапазоне от 0 до 7.
------------------	--

По умолчанию

Значение по умолчанию – 5.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для маркировки CoS пакетов Surveillance, поступающих на порт, на котором включена Surveillance VLAN. Маркировка CoS позволяет отделить трафик Surveillance VLAN от трафика данных по качеству обслуживания.

Пример

В данном примере показано, как настроить приоритет Surveillance VLAN со значением 7.

```
Switch# configure terminal
Switch(config)# surveillance vlan qos 7
Switch(config)#
```

88-6 show surveillance vlan

Данная команда используется для отображения настроек Surveillance VLAN.

```
show surveillance vlan [interface [INTERFACE-ID [, | -]]]
show surveillance vlan device [interface [INTERFACE-ID [, | -]]]
```

Параметры

device	Укажите, чтобы отобразить информацию об изученных устройствах Surveillance.
interface	(Опционально) Укажите, чтобы отобразить информацию о Surveillance VLAN на портах.
<i>INTERFACE-ID</i>	(Опционально) Укажите порт, о котором необходимо отобразить информацию.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду для отображения настроек Surveillance VLAN.

Для отображения глобальных настроек Surveillance VLAN используйте команду **show surveillance vlan**. Для отображения настроек Surveillance VLAN на интерфейсах используйте команду **show surveillance vlan interface**. Для отображения устройства Surveillance, информация о котором была получена через OUI, используйте команду **show surveillance vlan device**.

Пример

В данном примере показано, как отобразить глобальные настройки Surveillance VLAN.

```
Switch#show surveillance vlan
```

```
Surveillance VLAN ID : 1001  
Surveillance VLAN CoS : 5  
Aging Time           : 30 minutes  
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#
```

89. Команды портов коммутатора

89-1 duplex

Данная команда используется для настройки режима дуплекса на интерфейсе физического порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
duplex {full | auto} [rj45 | sfp]
no duplex [rj45 | sfp]
```

Параметры

full	Укажите для работы порта в режиме полного дуплекса (Full-Duplex Mode).
auto	Укажите, чтобы режим дуплекса на порту был определен автосогласованием (Auto-Negotiation).
rj45	(Опционально) Укажите, чтобы настроить режим дуплекса для среды передачи данных порта RJ-45. Для комбо-портов: если порт не указан, по умолчанию будет использован RJ-45.
sfp	(Опционально) Укажите, чтобы настроить режим дуплекса для среды передачи данных порта SFP.

По умолчанию

Для интерфейсов 100Base-TX и 1000Base-T параметр по умолчанию – **auto**.
Для интерфейсов 100Base-FX и 1000Base-SX/LX параметр по умолчанию – **full**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

На интерфейсе 100Base-FX устанавливается скорость 10 Мбит/с и режим полного дуплекса. На интерфейсе 1000Base-SX/LX устанавливается скорость 100 Мбит/с и режим полного дуплекса.

Данная команда не поддерживается модулями 100Base-FX и 1000Base-SX/LX.

Чтобы включить функцию автосогласования, необходимо указать параметр **auto** или для скорости, или для режима дуплекса. При фиксированном значении режима дуплекса и указании параметра **auto** для скорости будет согласована только скорость. Может быть установлена любая скорость в зависимости от выбранного режима дуплекса. При фиксированном значении скорости и указании параметра **auto** для режима дуплекса будет согласован только режим дуплекса.

Пример

В данном примере показано, как установить фиксированную скорость 100 Мбит/с и настроить режим дуплекса, определенный автосогласованием, на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# speed 100
Switch(config-if)# duplex auto
Switch(config-if)#
```

89-2 flowcontrol

Данная команда используется для настройки возможности управления потоком (Flow Control) на интерфейсе порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

flowcontrol {on | off}
no flowcontrol

Параметры

on	Укажите, чтобы включить на порту отправку или обработку кадров PAUSE, поступающих из удаленных портов.
off	Укажите, чтобы отключить отправку или не получать кадры PAUSE.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

С помощью данной команды можно настроить возможность управления потоком только в программном обеспечении коммутатора. Фактическая операция, выполняемая средствами аппаратного обеспечения, может отличаться от заданной, так как возможность управления потоком настраивается как на текущем, так и на удаленном порту/устройстве.

При установлении фиксированной скорости заданная настройка управления потоком будет окончательной. При установлении скорости, определенной автосогласованием, окончательная примененная настройка управления потоком будет основана на согласовании настроек локального устройства и коммутатора. В данном случае настройка управления потоком осуществляется с помощью локального устройства.

Данная команда не поддерживается коммутаторами, объединенными в физический стек.

Пример

В данном примере показано, как включить управление потоком на интерфейсе Ethernet 1/0/1.


```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# flowcontrol on
Switch(config-if)#
```

89-3 mdix

Данная команда используется для настройки состояния MDIX порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
mdix {auto | normal | cross}
no mdix
```

Параметры

auto	Укажите, чтобы включить режим Auto-MDIX Mode.
normal	Укажите, чтобы включить режим Normal Mode.
cross	Укажите, чтобы включить режим Cross Mode.

По умолчанию

Режим по умолчанию – Auto-MDIX Mode.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда неприменима на порту, к которому подключен оптоволоконный кабель.

Пример

В данном примере показано, как настроить режим Auto-MDIX Mode на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#mdix auto
Switch(config-if)#
```

89-4 speed

Данная команда используется для настройки скорости интерфейса физического порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.



Примечание: скорости 10 Мбит/с и 100 Мбит/с недоступны на портах 10G.

`speed {10 | 100 | 1000 [master | slave] | 10giga [master | slave] | auto [SPEED-LIST]} [rj45 | sfp]
no speed [rj45 | sfp]`

Параметры

10	Укажите, чтобы установить скорость 10 Мбит/с.
100	Укажите, чтобы установить скорость 100 Мбит/с.
1000	Укажите, чтобы установить скорость 1000 Мбит/с на медных портах. Необходимо вручную задать статус порта: Master (основное устройство) или Slave (дополнительное устройство). Укажите, чтобы отключить автосогласование на всех оптических портах (1000Base-SX/LX).
master slave	Укажите статус порта: Master (основное устройство) или Slave (дополнительное устройство). Данный параметр применим только к устройствам, подключенным к порту 1000Base-T.
10giga	Укажите, чтобы установить скорость 10 Гбит/с.
master slave	Укажите статус порта: Master (основное устройство) или Slave (дополнительное устройство). Данный параметр применим только к устройствам, подключенным к порту 10GBase-T.
auto	Укажите, чтобы скорость и управление потоком медных портов с оборудованием на противоположной стороне были заданы при помощи автосогласования. Укажите, чтобы включить на оптических портах (1000Base-SX/LX) функцию автосогласования, с помощью которой время и управление потоком будут согласованы с оборудованием на противоположной стороне.
SPEED-LIST	(Опционально) Укажите список скоростей, применяемых для автосогласования. Возможны следующие скорости: 1000 и/или 10giga . Если используются несколько скоростей, необходимо отделить их запятой (,). Если список скоростей не указан, будут анонсированы все варианты скорости.
rj45	(Опционально) Укажите, чтобы настроить скорость передачи данных для порта RJ-45. Для комбо-портов: если порт не указан, по умолчанию будет использован RJ-45.
sfp	(Опционально) Укажите, чтобы настроить скорость передачи данных для порта SFP/SFP+.

По умолчанию

Для интерфейсов 100Base-TX, 1000Base-T и 10GBase-T по умолчанию скорость определяется автоматически.
Для интерфейсов 100Base-FX по умолчанию устанавливается фиксированная скорость 100 Мбит/с.
Для интерфейсов 1000Base-SX/LX по умолчанию устанавливается фиксированная скорость 1000 Мбит/с.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если указанная скорость не поддерживается аппаратно, будет отображено сообщение об ошибке. На устройстве с интерфейсом 100Base-FX всегда устанавливается фиксированная скорость 100 Мбит/с и режим полного дуплекса. Данный интерфейс не поддерживает функцию автосогласования. Изменить настройки данного интерфейса нельзя ни одной командой. На устройстве с интерфейсом 1000Base-SX/LX всегда устанавливается фиксированная скорость 1000 Мбит/с и режим полного дуплекса. Для данного интерфейса доступны только команды **speed 1000** и **speed auto**. Если на порту 1000Base-T установлена скорость подключения 1000 Мбит/с, а на порту 10GBase-T – 10 Гбит/с, необходимо задать статус для данных портов: Master (основное устройство) или Slave (дополнительное устройство).

Чтобы включить функцию автосогласования, необходимо указать параметр **auto** или для скорости, или для режима дуплекса. При фиксированном режиме дуплекса и указании параметра **auto** для скорости будет согласована только скорость. Может быть установлена любая скорость в зависимости от выбранного режима дуплекса. При фиксированной скорости и указании параметра **auto** для режима дуплекса будет согласован только режим дуплекса.

При включенной функции автосогласования на порту 10GBase-R автоматически будет установлена скорость подключения в зависимости от типа SFP/SFP+ (1000 Мбит/с или 10 Гбит/с).

Пример

В данном примере показано, как на интерфейсе Ethernet 1/0/1 включить автосогласование, при котором будут использоваться только скорости 10 Мбит/с или 100 Мбит/с.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# speed auto 10,100
Switch(config-if)#
```

90. Команды управления системных файлов

90-1 boot config

Данная команда используется для указания конфигурационного файла, который будет использован при следующем запуске устройства.

boot config *URL*

Параметры

<i>URL</i>	Укажите URL конфигурационного файла, который будет использован при следующем запуске устройства.
------------	--

По умолчанию

По умолчанию используется файл **config.cfg**.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы указать конфигурационный файл, который будет использован при следующем запуске устройства. При отсутствии конфигурационного файла устройство вернется к настройкам по умолчанию.

Пример

В данном примере показано, как указать конфигурационный файл «switch-config.cfg», который будет использован при следующем запуске устройства.

```
Switch# configure terminal
Switch(config)# boot config c:/switch-config.cfg
Switch(config)#
```

90-2 boot image

Данная команда используется для указания файла образа, который будет использован при следующем запуске устройства.

boot image [**check**] *URL*

Параметры

check	(Опционально) Укажите данный параметр для отображения
--------------	---

	информации о программном обеспечении для указанного файла (номер версии и описание модели).
<i>URL</i>	Укажите URL файла образа для загрузки.

По умолчанию

По умолчанию используется один файл образа для загрузки.

Режим ввода команды**Global Configuration Mode****Уровень команды по умолчанию**

Уровень 15

Использование команды

Используйте данную команду, чтобы указать файл образа, который будет использован при следующем запуске устройства. После проверки и утверждения системой модели и контрольной суммы файл образа будет допущен.

Используйте параметр **check**, чтобы проверить может ли быть допущен указанный файл образа для загрузки. Настройка команды **boot image** будет сохранена в энергонезависимой памяти NVRAM, благодаря которой сохраненный файл будет использован при следующем запуске устройства.

Образ резервного копирования определяется автоматически. Обычно ранее загруженный образ заменяется новым.

Пример

В данном примере показано, как указать файл под именем «switch-image1.had» в качестве файла образа для загрузки.

```
Switch# configure terminal
Switch(config)# boot image c:/switch-image1.had
Switch(config)#
```

В данном примере показано, как проверить указанный файл образа с именем «c:/runtime.switch.had». Информация о файле будет отображена после подтверждения его контрольной суммы.

```
Switch#configure terminal
Switch(config)#boot image check c:/runtime.wrongswitch.had

-----
Image information
-----
Version: 1.00.001
Description: D-Link Corporation TenGigabit Ethernet Switch

Switch(config)#
```

В данном примере показано, как проверить указанный файл образа с именем «runtime.wrongswitch.had». Контрольная сумма данного файла не прошла проверку, поэтому отобразилось сообщение об ошибке.

```
Switch# configure terminal
Switch(config)# boot image check runtime.wrongswitch.had
ERROR: Invalid firmware image.
Switch(config)#
```

90-3 clear running-config

Данная команда используется для удаления текущей конфигурации системы (running configuration).

clear running-config

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы удалить конфигурацию системы, сохраненную в DRAM-память. Данные конфигурации вернуться 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#
```

90-4 reset system

Данная команда используется для сброса системы и удаления ранее сохраненной конфигурации с дальнейшей перезагрузкой коммутатора.

reset system

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для удаления конфигурации системы, включая информацию о стеке. Данные конфигурации вернутся к настройкам по умолчанию, будет создан соответствующий конфигурационный файл загрузки, затем будет выполнен перезапуск коммутатора. Перед использованием данной команды сохраните резервную копию конфигурации с помощью команды **copy** или выгрузите профиль конфигурации на TFTP-сервер.

Пример

В данном примере показано, как сбросить систему и вернуться к настройкам по умолчанию.

```
Switch#reset system

This command will clear the system's configuration to the factory
default settings, including the IP address and stacking settings.
Clear system configuration, save, reboot? (y/n) [n] y
Saving configurations and logs to NV-RAM..... Done
Please wait, the switch is rebooting...
```

90-5 configure replace

Данная команда используется для замены текущей конфигурации указанным конфигурационным файлом.

configure replace **{tftp: //location/filename | flash: FILENAME}** **[force]**

Параметры

tftp: Укажите конфигурационный файл с TFTP-сервера.

<code>//location/filename</code>	Укажите URL конфигурационного файла на TFTP-сервере.
flash:	Укажите, что конфигурационный файл из NVRAM.
<code>FILENAME</code>	Укажите имя конфигурационного файла, хранящегося в NVRAM.
force	(Опционально) Укажите, чтобы принудительно применить команду без дополнительного подтверждения.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду, чтобы заменить текущую конфигурацию указанным конфигурационным файлом. Текущая конфигурация будет удалена перед применением указанной конфигурации.



Примечание: при выполнении данной команды текущая конфигурация полностью меняется на конфигурацию указанного файла. В указанном конфигурационном файле должна быть представлена полная конфигурация, а не частичная.

Перед использованием данной команды сохраните резервную копию конфигурации с помощью команды **сору** или выгрузите профиль конфигурации на TFTP-сервер.

Пример

В данном примере показано, как заменить текущую конфигурацию файлом «config.cfg», загруженным с TFTP-сервера.

```
Switch# configure replace tftp: //10.0.0.66/config.cfg

This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. [y/n]: y

Accessing tftp://10.0.0.66/config.cfg...
Transmission start...
Transmission finished, file length 45422 bytes.
Executing script file config.cfg .....
Executing done

Switch#
```


В данном примере показано, как заменить текущую конфигурацию файлом «config.cfg», хранящимся в NVRAM. Команда выполняется принудительно без дополнительного подтверждения.

```
Switch# configure replace flash: config.cfg force

Executing script file config.cfg .....
Executing done

Switch#
```

90-6 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>	<p>Укажите URL источника исходного файла, который необходимо скопировать. Особые формы URL представлены следующими ключевыми словами:</p> <p>Укажите startup-config в качестве URL источника, чтобы выгрузить конфигурацию, которая будет применена после запуска коммутатора, сохранить ее как файл в файловой системе или использовать в качестве текущей конфигурации.</p> <p>Укажите running-config в качестве URL источника, чтобы выгрузить текущую конфигурацию, сохранить ее в качестве загрузочной конфигурации или как файл в файловой системе.</p> <p>Укажите flash: [PATH-FILE-NAME] в качестве URL источника, чтобы скопировать исходный файл в файловую систему.</p> <p>Укажите log в качестве URL, чтобы выгрузить системный журнал на TFTP-сервер или сохранить его как файл в файловую систему.</p> <p>Укажите attack-log UNIT-ID в качестве URL источника, чтобы выгрузить журнал атак указанного Unit.</p>
<i>DESTINATION-URL</i>	<p>Укажите URL назначения скопированного файла. Особые формы URL представлены следующими ключевыми словами:</p> <p>Укажите running-config в качестве URL назначения, чтобы применить конфигурацию к текущей конфигурации.</p> <p>Укажите startup-config в качестве URL назначения, чтобы сохранить конфигурацию, которую необходимо применить при следующем запуске. Текущая конфигурация будет сохранена в NVRAM, а имя файла будет совпадать с именем файла, указанным при использовании команды bootconfig.</p> <p>Укажите flash: [PATH-FILE-NAME] в качестве URL назначения, чтобы указать имя копируемого файла в</p>

	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).
<i>LOCATION</i>	Укажите IPv4-адрес TFTP/FTP/RCP-сервера или IPv6-адрес TFTP/FTP- сервера.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Используйте данную команду для копирования файлов в файловую систему, загрузки/выгрузки конфигурационного файла или файла образа, загрузки системного журнала на TFTP-сервер. Чтобы выгрузить текущую конфигурацию или сохранить ее в качестве загрузочной конфигурации, укажите **running-config** в качестве URL источника. Чтобы сохранить текущую конфигурацию в качестве загрузочной конфигурации, укажите **startup-config** в качестве URL назначения.

Если в качестве назначения указана загрузочная конфигурация, файл исходника будет скопирован в файл, указанный в команде **boot config**. Исходный файл загрузочной конфигурации будет перезаписан.

Чтобы применить необходимый конфигурационный файл к текущей конфигурации, при использовании команды **copy** укажите **running-config** в качестве URL назначения. Данный конфигурационный файл будет сразу же применен, используя метод Increment. Указанная конфигурация будет объединена с текущей конфигурацией. Текущая конфигурация будет удалена только после применения указанной конфигурации.

Если в качестве источника указан системный журнал, а в качестве назначения указан URL, текущий системный журнал будет скопирован на указанный URL.

Чтобы отобразить файл на удаленном TFTP-сервере, необходимо использовать URL с префиксом «tftp://».

Чтобы загрузить образ программного обеспечения, используйте команду **copy tftp://** для загрузки файла с TFTP-сервера в файловую систему. Чтобы указать данный файл в качестве файла образа для загрузки, используйте команду **boot image**.

Пример

В данном примере показано, как применить на коммутаторе конфигурацию как текущую, загруженную с TFTP-сервера, используя метод Increment. Имя конфигурационного файла: switch-config.cfg. TFTP- сервер: 10.1.1.254.

```
Switch# copy tftp: //10.1.1.254/switch-config.cfg running-config

Address of remote host []? 10.1.1.254
Source filename []? switch-config.cfg
Destination filename running-config? [y/n]: y

  Accessing tftp://10.1.1.254/switch-config.cfg...
  Transmission start...
  Transmission finished, file length 45421 bytes.
  Executing script file switch-config.cfg .....
  Executing done

Switch#
```

В данном примере показано, как выгрузить текущую конфигурацию на TFTP-сервер для хранения.

```
Switch# copy running-config tftp: //10.1.1.254/switch-config.cfg

Address of remote host []? 10.1.1.254
Destination filename []? switch-config.cfg
  Accessing tftp://10.1.1.254/switch-config.cfg...
  Transmission start...
  Transmission finished, file length 45421 bytes.

Switch#
```

В данном примере показано, как сохранить текущую конфигурацию во FLASH-память и использовать ее при следующем запуске устройства.

```
Switch# copy running-config startup-config

Destination filename startup-config? [y/n]: y

Saving all configurations to NV-RAM..... Done.

Switch#
```

В данном примере показано, как немедленно сохранить файл «switch-config.cfg» в NVRAM, используя метод Increment.

```
Switch# copy flash: switch-config.cfg running-config

Source filename [switch-config.cfg]?
Destination filename running-config? [y/n]: y

  Executing script file switch-config.cfg .....
  Executing done

Switch#
```

В данном примере показано, как загрузить файл образа с TFTP-сервера на все устройства в стеке.

```

Switch# copy tftp: //10.1.1.254/image.had flash: image.had

Address of remote host [10.1.1.254]?
Source filename [image.had]?
Destination filename [image.had]?
Accessing tftp://10.1.1.254/image.had...
Transmission start...
Transmission finished, file length 8315060 bytes.
Transmission to slave start..... Done.
Transmission to slave finished, file length 8315060 bytes.
Please wait, programming flash..... Done.
Wait slave programming flash complete...
Done.

Switch#

```

90-7 ip tftp source-interface

Данная команда используется для указания интерфейса, IP-адрес которого будет использоваться в качестве адреса источника для инициирования TFTP-пакетов. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```

ip tftp source-interface INTERFACE-ID
no ip tftp source-interface

```

Параметры

<i>INTERFACE-ID</i>	Укажите IP-адрес интерфейса, который будет использоваться в качестве адреса источника для инициирования TFTP-пакетов.
---------------------	---

По умолчанию

По умолчанию используется IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для указания интерфейса, IP-адрес которого будет использоваться в качестве адреса источника для инициирования TFTP-пакетов. Чтобы загрузить программное обеспечение через порт управления Out-Of-Band Management Port, укажите ID интерфейса данного порта.

Данная команда поддерживает только интерфейсы Loopback, MGMT и VLAN.

Пример

В данном примере показано, как загрузить программное обеспечение через порт управления Out-Of- Band.

```
Switch# configure terminal
Switch(config)# ip tftp source-interface mgmt0
Switch(config)#
```

90-8 show boot

Данная команда используется для отображения настроек конфигурационного файла и загрузочного образа.

show boot [unit *UNIT-ID*]

Параметры

<i>UNIT-ID</i>	(Опционально) Укажите модуль (Unit), который необходимо отобразить.
----------------	---

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Команда используется для отображения настроек конфигурационного файла и загрузочного образа.

Пример

В данном примере показано, как отобразить информацию о загрузке системы.

```
Switch# show boot

Unit 1
Boot image: c:/bootimage.had
Boot config: c:/def_usr.cfg

Unit 2
Boot image: c:/bootimage.had
Boot config: c:/def_usr.cfg

Switch#
```

90-9 show running-config

Данная команда используется для отображения команд текущего конфигурационного файла.

show running-config

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Команда используется для отображения текущей конфигурации.

Пример

В данном примере показано, как отобразить содержимое текущего конфигурационного файла.

```
Switch#show running-config
Building configuration...

Current configuration : 37947 bytes

#-----
#                               DGS-3130-30TS Gigabit Ethernet Switch
#                               Configuration
#
#                               Firmware: Build 1.00.001
#                               Copyright(C) 2017 D-Link Corporation. All rights reserved.
#-----

# STACK

end

# DEVICE

# AAA

configure terminal
# AAA START
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

90- 10 show startup-config

Данная команда используется для отображения содержимого конфигурационного загрузочного файла.

show startup-config

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 15

Использование команды

Команда используется для отображения настроек конфигурации, с помощью которых система будет инициализирована.

Пример

В данном примере показано, как отобразить содержимое конфигурационного загрузочного файла.

```
Switch#show startup-config
```

```
#-----  
#  
#           DGS-3130-30TS Gigabit Ethernet Switch  
#           Configuration  
#  
#           Firmware: Build 1.00.001  
#           Copyright(C) 2017 D-Link Corporation. All rights reserved.  
#-----
```

```
# STACK
```

```
end
```

```
end
```

```
# DEVICE
```

```
# AAA
```

```
configure terminal
```

```
# AAA START
```

```
no aaa new-model
```

```
# AAA END
```

```
CTRL+C BSC q Quit SPACE n Next Page ENTER Next Entry a All
```


91. Команды System Log

91-1 clear logging

Данная команда используется для удаления сообщений логирования из буфера системного логирования.

clear logging

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда позволяет удалить все записи логирования из буфера системного логирования.

Пример

В данном примере показано, как удалить все записи логирования из буфера системного логирования.

```
Switch# clear logging
Clear logging? (y/n) [n] y
Switch#
```

91-2 logging on

Данная команда используется для включения логирования системных сообщений. При использовании формы no команда отключит логирование системных сообщений.

logging on
no logging on

Параметры

Нет

По умолчанию

По умолчанию опция включена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Для включения логирования системных сообщений используйте команду **logging on** в режиме Global Configuration Mode. Данная команда отправляет сообщения об отладке (debug) или ошибке (error) в процессе логирования, при котором сохраняются сообщения асинхронно с процессом, генерирующим данные сообщения. Используйте форму **no** для отключения процесса логирования.

Процесс логирования управляет распределением сообщений логирования на различные точки назначения, например, буфер логирования, сессии терминала, сервер syslog. Сообщения системного логирования также известны как сообщения системных ошибок. Логирование можно включить и отключить для каждой из точек назначения индивидуально, используя команды **logging buffered**, **logging server** и **logging global configuration**. Однако если отключена команда **logging on**, сообщения на данные точки назначения отправляться не будут. Если команда **logging on** включена, одновременно будет включен **logging buffered**.

Пример

В данном примере показано, как включить логирование системных сообщений.

```
Switch# configure terminal
Switch(config)# logging on
WARNING: The command takes effect and the logging buffered is enabled at the same time.
Switch(config)#
```

91-3 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

<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 (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: emergencies (0), alerts (1), critical (2), errors (3), warnings (4), notifications (5), informational (6), debugging (7) .
discriminator	(Опционально) Укажите discriminator для фильтрации сообщений, отправляемых в локальный буфер.
write-delay SECONDS	(Опционально) Укажите задержку периодической записи буфера логирования во FLASH-память на указанное количество секунд.

По умолчанию

По умолчанию используется уровень важности warning (4).

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Системные сообщения можно логировать в локальный буфер сообщений, локальную консоль или в другие места. Сообщения должны быть введены в локальный буфер сообщений перед отправкой в другие точки назначения.

Команда не будет применена, если указанный discriminator не существует. В таком случае будут применяться настройки по умолчанию.

Укажите уровень важности сообщений для ограничения системных сообщений, логируемых в буфер (это позволит уменьшить число логируемых 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)#
```

91-4 logging console

Данная команда используется для включения логирования системных сообщений в локальной консоли. При использовании формы **no** команда отключит логирование сообщений в локальной консоли и вернет настройки по умолчанию.

logging console [severity {SEVERITY-LEVEL | SEVERITY-NAME}] [discriminator NAME]
no logging console

Параметры

<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 (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: emergencies (0), alerts (1), critical (2), errors (3), warnings (4), notifications (5), informational (6), debugging (7).
discriminator	(Опционально) Укажите discriminator для фильтрации сообщений, отправляемых в локальный буфер.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Системные сообщения можно логировать в локальный буфер сообщений, локальную консоль или другие точки назначения. Сообщения должны быть введены в локальный буфер сообщений перед отправкой в консоль.

Команда не будет применена, если указанный discriminator не существует. В таком случае будут применяться настройки по умолчанию.

Укажите уровень важности сообщений для ограничения системных сообщений, логируемых в консоли. Сообщения указанного уровня или выше будут логироваться в локальную консоль.

Пример

В данном примере показано, как включить логирование сообщений в локальную консоль и ограничить логирование сообщений с уровнем важности errors или выше.

```
Switch# configure terminal
Switch(config)# logging console severity errors
Switch(config)#
```

91-5 logging discriminator

Данная команда используется при создании discriminator для дальнейшей фильтрации сообщений SYSLOG, отправляемых в различные точки назначения. При использовании формы по 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.
facility	(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.
includes	Укажите для включения совпадающих сообщений. Несовпадающие сообщения будут фильтроваться.
drops	Укажите для фильтрации совпадающих сообщений.
severity	(Опционально) Укажите подфильтр на основе совпадений с уровнем важности.
<i>SEVERITY-LIST</i>	Укажите список уровней важности для фильтрации или включения.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Настройка существующего параметра discriminator. При вводе команды более ранние настройки будут переписаны на новые. Ассоциируйте discriminator с командами logging buffered и logging server.

Пример

В данном примере показано, как создать discriminator с именем «buffer-filter», указывающим два подфилтра, 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)#
```

91-6 logging server

Данная команда используется для создания серверного узла SYSLOG для логирования системных сообщений или вывода при отладке. При использовании формы **no** команда удалит серверный узел SYSLOG.

logging server {*IP-ADDRESS* | *IPV6-ADDRESS*} [**severity** {*SEVERITY-LEVEL* | *SEVERITY-NAME*}] [**facility** {*FACILITY-NUM* | *FACILITY-NAME*}] [**discriminator** *NAME*] [**port** *UDP-PORT*]
no logging server {*IP-ADDRESS* | *IPV6-ADDRESS*}

Параметры

<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 (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: emergencies (0), alerts (1), critical (2), errors (3), warnings (4), notifications (5), informational (6), debugging (7).
<i>FACILITY-NUM</i>	(Опционально) Укажите десятичное значение от 0 до 23 для facility. Если значение не указано, по умолчанию будет использоваться local7 (23). Для более подробной информации обратитесь к параграфу Использование команды .
<i>FACILITY-NAME</i>	(Опционально) Укажите имя для facility. Если значение не

	указано, по умолчанию будет использоваться local7 (23). Для более подробной информации обратитесь к параграфу Использование команды .
discriminator NAME	(Опционально) Укажите для фильтрации сообщений на сервер логирования согласно настройке discriminator.
port UDP-PORT	(Опционально) Укажите номер порта UDP, который будет использоваться сервером SYSLOG. Доступен диапазон значений от 1024 до 65535, а также 514 (распространенный порт IANA). Если значение не указано, номер UDP-порта по умолчанию – 514.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Системные сообщения можно логировать в локальный буфер сообщений, локальную консоль или на удаленные узлы. Сообщения должны быть введены в локальный буфер сообщений перед отправкой на сервер логирования.

Ниже представлена таблица значений Facility.

Номер Facility	Имя Facility	Описание
0	kern	Сообщения ядра
1	user	Сообщения уровня пользователя
2	mail	Система почты
3	daemon	Системные daemon
4	auth1	Сообщения системы безопасности/авторизации
5	syslog	Сообщения, генерируемые SYSLOG
6	lpr	Подсистема Line Printer
7	news	Подсистема сетевых новостей
8	uucp	Подсистема UUCP
9	clock1	Clock daemon
10	auth2	Сообщения системы безопасности/авторизации
11	ftp	FTP daemon
12	ntp	Подсистема NTP
13	logaudit	Аудит логирования
14	logalert	Предупреждение логирования
15	clock2	Clock daemon (note 2)

16	local0	Локальное использование 0 (local0)
17	local1	Локальное использование 1 (local1)
18	local2	Локальное использование 2 (local2)
19	local3	Локальное использование 3 (local3)
20	local4	Локальное использование 4 (local4)
21	local5	Локальное использование 5 (local5)
22	local6	Локальное использование 6 (local6)
23	local7	Локальное использование 7 (local7)

Пример

В данном примере показано, как включить логирование системных сообщений с уровнем важности выше warnings на удаленном узле 20.3.3.3.

```
Switch# configure terminal
Switch(config)# logging server 20.3.3.3 severity warnings
Switch(config)#
```

91-7 logging smtp

Данная команда используется для включения логирования системных сообщений получателям электронной почты. При использовании формы **no** команда отменит логирование системных сообщений получателям электронной почты и вернется к настройкам по умолчанию.

logging smtp [severity {SEVERITY-LEVEL /SEVERITY-NAME}] [discriminator NAME]
no logging smtp

Параметры

<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 (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: emergencies (0), alerts (1), critical (2), errors (3), warnings (4), notifications (5), informational (6), debugging (7).
discriminator NAME	(Опционально) Укажите для фильтрации сообщений, отправляемых на почту, на основе значения discriminator.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Системные сообщения можно логировать на электронную почту. Данная команда не будет применена, если указанный discriminator не существует. В таком случае будут применяться настройки по умолчанию. Сообщения необходимо логировать в локальный буфер перед отправкой на электронную почту.

Укажите уровень важности сообщений для ограничения системных логируемых сообщений. Сообщения указанного уровня или выше будут логироваться на электронную почту.

Пример

В данном примере показано, как включить логирование системных сообщений с уровнем важности выше warnings на электронную почту.

```
Switch# configure terminal
Switch(config)# logging smtp severity warnings
Switch(config)#
```

91-8 logging source-interface

Данная команда используется для указания IP-адреса интерфейса, который будет использоваться в качестве адреса источника для отправки пакетов SYSLOG. При использовании формы **no** команда вернется к настройкам по умолчанию.

logging source-interface *INTERFACE-ID*
no logging source-interface

Параметры

<i>INTERFACE-ID</i>	Укажите IP-адрес интерфейса, который будет использоваться в качестве адреса источника для отправки пакетов SYSLOG.
---------------------	--

По умолчанию

По умолчанию используется IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для указания IP-адреса интерфейса, который будет использоваться в качестве адреса источника для отправки пакетов SYSLOG.

Для команды поддерживаются только интерфейсы Loopback, MGMT и VLAN.

Пример

В данном примере показано, как настроить VLAN 100 в качестве интерфейса источника для пакетов SYSLOG.

```
Switch# configure terminal
Switch(config)# logging source-interface vlan 100
Switch(config)#
```

91-9 show logging

Данная команда используется для просмотра системных сообщений, логированных в локальном буфере.

show logging [all | [REF-SEQ] [+ NN | - NN]]

Параметры

all	(Опционально) Укажите для отображения всех записей лога, начиная с последних.
REF-SEQ	(Опционально) Укажите для отображения с номера, следующего за указанным.
+ NN	(Опционально) Укажите количество сообщений, появившихся после указанного номера, следующим за указанным. Если значение не указано, отображение начинается от самых давних сообщений в буфере.
- NN	(Опционально) Укажите количество сообщений, появившихся до указанного номера, следующим за указанным. Если значение не указано, отображение начинается от самых последних сообщений в буфере.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Команда используется для просмотра системных сообщений, логированных в локальном буфере.

Каждое логированное в буфер сообщение ассоциировано с номером последовательности. При логировании сообщения назначается номер последовательности, начиная с 1. Номер последовательности вернется к 1 после достижения 100000.

Если пользователь указывает отображение количества сообщений после номера, следующим за указанным, более поздние сообщения будут отображаться до новых. Если пользователь указывает отображение количества сообщений с номера, следующим за указанным, новые сообщения будут отображаться до более поздних.

Если команда введена без опций, будет отображено 200 записей, начиная от самых последних.

Пример

В данном примере показано, как отобразить сообщения в локальном буфере сообщений.

```
Switch# show logging
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#
```

91-10 show attack-logging

Данная команда используется для просмотра логированных сообщений об атаках.

show attack-logging unit *UNIT-ID* [index *INDEX*]

Параметры

<i>UNIT-ID</i>	Укажите модуль (Unit), для которого необходимо отобразить логированные сообщения об атаке.
index <i>INDEX</i>	Укажите список номеров index-записей, которые необходимо отобразить. Если значение не указано, отображаться будут все данные из журнала атак.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для просмотра логированных сообщений журнала об атаках. Такие сообщения относятся к сообщениям журнала, управляемым такими модулями, как DOS и port-security. Данный тип логированных сообщений может генерировать большое число сообщений, из-за чего в системе быстро закончится память для логирования. Поэтому для данного типа сообщений в системном журнале хранится только первое логирование, генерируемое каждую минуту, а остальные хранятся в отдельной таблице с именем attack log (журнал атак).

Пример

В данном примере показано, как отобразить первое логированное сообщение об атаке.

```
Switch# show attack-logging index 1
Attack log messages:
1 2015-03-24 15:00:14 CRIT(2) Land attack is blocked from (IP: 10.72.24.1 Port: 7)
Switch#
```

9-11 clear attack-logging

Данная команда используется для удаления сообщений об атаках.

clear attack-logging {unit UNIT-ID | all}

Параметры

unit UNIT-ID	Укажите модуль (Unit), для которого необходимо удалить логированные сообщения об атаке.
all	Укажите для удаления всех записей.

По умолчанию

Нет

Режим ввода команды

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для удаления сообщений об атаках.

Пример

В данном примере показано, как удалить все логированные сообщения об атаках.

```
Switch# clear attack-logging all
Switch#
```

92. Команды времени и SNTP

92-1 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

Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Если система синхронизируется с помощью любого действующего внешнего механизма синхронизации, такого как SNTP, необходимо установить системное время. Используйте данную команду, если другие источники времени недоступны. Время, указанное в данной команде, принадлежит к часовому поясу, заданному конфигурацией команды **clock timezone**. Если устройство поддерживает функцию RTC (часы реального времени), время синхронизируется с RTC. Настроенные часы не будут сохранены в файле конфигурации.

Сервер SNTP является основным источником времени: даже если системное время было настроено вручную, при подключении к серверу SNTP время будет синхронизировано с его показателями.

Пример

В данном примере показано, как вручную установить системное время на 18:00, 4 июля 2013 г.

```
Switch# clock set 18:00:00 4 Jul 2013
Switch#
```

92-2 clock summer-time

Данная команда используется для настройки автоматического перехода на летнее время. Используйте форму **no**, чтобы отключить автоматический переход на летнее время.

clock summer-time recurring WEEK DAY MONTH HH:MM WEEK DAY MONTH HH:MM [OFFSET]
clock summer-time date DATE MONTH YEAR HH:MM DATE MONTH YEAR HH:MM [OFFSET]
no clock summer-time

Параметры

recurring	Укажите дату начала и окончания летнего времени (день недели и месяц).
date	Укажите точную дату начала и окончания летнего времени.
<i>WEEK</i>	Укажите номер недели месяца (от 1 до 4) или слово «last», с помощью которого будет указана последняя неделя месяца.
<i>DAY</i>	Укажите день недели (sun, mon и т. д.).
<i>DATE</i>	Укажите день месяца (от 1 до 31).
<i>MONTH</i>	Укажите порядковый номер месяца в диапазоне от 1 до 12, где 1 – это январь, 2 – февраль и т. д.
<i>YEAR</i>	Укажите года, чтобы задать необходимый интервал для применения перехода на летнее время.
<i>HH:MM</i>	Укажите время (24-часовой формат) в часах и минутах.
<i>OFFSET</i>	(Опционально) Укажите количество минут, которое нужно добавить при переходе на летнее время. Значение по умолчанию – 60. Доступный диапазон смещения – 30, 60, 90 и 120 минут.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы перейти на летнее время автоматически. У команды две формы: первая – повторяющаяся (**recurring**), которая используется для указания даты начала и окончания летнего времени (день недели и месяц); вторая – форма даты (**date**), которая используется для указания определенного числа месяца.

Первая часть данных команд указывает на начало летнего времени, а вторая – на конец.

Пример

В данном примере показано, как назначить начало летнего времени на 2 часа ночи первого воскресенья апреля и конец на 2 часа ночи последнего воскресенья октября.

```
Switch# configure terminal
Switch(config)# clock summer-time recurring 1 sun 4 2:00 last sun 10 2:00
Switch(config)#
```

92-3 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Время, полученное с сервера SNTP, синхронизируется с форматом UTC. При настройке местного времени учитывается формат UTC, часовой пояс и настройки перехода на летнее время.

Пример

В данном примере показано, как настроить часовой пояс PST (Северноамериканское Тихоокеанское Стандартное Время), который на 8 часов опережает время UTC.

```
Switch# configure terminal
Switch(config)# clock timezone - 8
Switch(config)#
```

92-4 show clock

Данная команда используется для отображения информации о времени и дате.

show clock

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Также данная команда используется для отображения источника времени. Возможные источники: «No Time Source» (источник времени отсутствует) или «SNTP».

Пример

В данном примере показано, как отобразить текущее время.

```
Switch#show clock

Current Time Source   : System Clock
Current Time         : 05:56:45, 2000-01-30
Time Zone            : UTC +00:00
Daylight Saving Time : Disabled

Switch#
```

92-5 show sntp

Данная команда используется для отображения информации о сервере SNTP.

show sntp

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode

Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения информации о сервере SNTP.

Пример

В данном примере показано, как отобразить информацию об SNTP.

```
Switch#show sntp

SNTP Status           : Enabled
SNTP Poll Interval    : 720 sec

SNTP Server Status:

SNTP Server           Version Last Receive
-----
10.0.0.11             4           00:02:02
10::2                 -----
FE80::1111vlan 1     -----
-----

Total Entries:3

Switch#
```

92-6 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

Уровень команды по умолчанию

Уровень 12

Использование команды

SNTP – это упрощенная клиентская версия NTP. В отличие от NTP, SNTP может получать время только от серверов NTP; его нельзя использовать для предоставления времени другим системам. SNTP обеспечивает время с погрешностью 100 миллисекунд от точного времени, но, в отличие от NTP, не 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)#
```

92-7 sntp enable

Данная команда используется для включения функции SNTP. Используйте форму **no**, чтобы отключить функцию SNTP.

```
sntp enable
no sntp enable
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для включения/отключения функции SNTP.

Пример

В данном примере показано, как включить функцию SNTP.

```
Switch# configure terminal
Switch(config)# sntp enable
Switch(config)#
```

92-8 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки интервала опроса (Polling Interval).

Пример

В данном примере показано, как настроить интервал на 100 секунд.

```
Switch# configure terminal
Switch(config)# sntp interval 100
Switch(config)#
```

93. Команды временного диапазона

93-1 periodic

Данная команда используется в режиме Time-Range Configuration Mode для указания профиля диапазона времени. Используйте форму **no**, чтобы удалить указанный временной диапазон.

periodic {daily HH:MM to HH:MM | weekly WEEKLY-DAY HH:MM to [WEEKLY-DAY] HH:MM}
no periodic {daily HH:MM to HH:MM | weekly WEEKLY-DAY HH:MM to [WEEKLY-DAY] HH:MM}

Параметры

daily HH:MM to HH:MM	Укажите время в формате ЧЧ:ММ (например, 18:30).
weekly WEEKLY-DAY HH:MM to [WEEKLY-DAY] HH:MM no:	Укажите день недели (monday, tuesday, wednesday, thursday, friday, saturday, sunday) и время в формате ЧЧ:ММ. Конечный день недели, совпадающий с начальным, можно не указывать.

По умолчанию

Нет

Режим ввода команды

Time-range Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Новый период может частично совпадать с предыдущим. Если начало и завершение нового периода соответствуют началу и завершению предыдущего периода, будет отображено сообщение об ошибке и новый период не будет задан. При удалении необходимо полностью указать заданный ранее период. Если период указан не полностью или указано сразу несколько периодов, будет отображено сообщение об ошибке.

Пример

В данном примере показано, как создать временной интервал, включающий промежутки с 09:00 до 12:00 ежедневно и с 00:00 субботы до 00:00 понедельника, а также как удалить период с 09:00 до 12:00 ежедневно.

```
Switch# configure terminal
Switch(config)# time-range rdtme
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)#
```

93-2 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

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Если параметр не указан, будут отображены все настроенные профили диапазона времени.

Пример

В данном примере показано, как отобразить все настроенные профили.

```
Switch#show time-range

Time Range Profile: lunchtime
Daily 12:00 to 13:00

Time Range Profile: rdttime
Weekly Saturday 00:00 to Monday 00:00
Daily 09:00 to 12:00

Total Entries :2

Switch#
```

93-3 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы войти в режим Time-Range Configuration Mode. Команду следует применять перед командой **periodic**, используемой для указания временного диапазона. Если временной диапазон создается без какой-либо настройки, это означает, что для данного временного диапазона нет активного периода, и отобразить его с помощью команды **show time-range** не получится.

Пример

В данном примере показано, как войти в режим Time-Range Configuration Mode для профиля диапазона времени с именем «rdtime».

```
Switch# configure terminal
Switch(config)# time-range rdtime
Switch(config-time-range)#
```

94. Команды Traffic Segmentation

94-1 show traffic-segmentation forward

Данная команда используется для отображения конфигурации Traffic Segmentation на указанных или всех портах.

```
show traffic-segmentation forward [interface INTERFACE-ID [, | -]]
```

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите интерфейсы, которые необходимо отобразить. Допустимый интерфейс: физический порт или port-channel.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Если параметр не указан, будет отображена конфигурация Traffic Segmentation для всех портов.

Пример

В данном примере показано, как отобразить конфигурацию Traffic Segmentation для интерфейса Ethernet 1/0/1.

```
Switch#show traffic-segmentation forward interface ethernet 1/0/1

Interface      Forwarding Domain
-----
eth1/0/1      eth1/0/3-1/0/6

Total Entries: 1

Switch#
```

94-2 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Если домен продвижения пакетов задан Traffic Segmentation, то пакеты, получаемые портом, будут ограничены пакетами, отправленными интерфейсами внутри заданного L2 домена. Если ограничение продвижения пакетов в домене L2 не указано, то получение портом пакетов не ограничено.

Команду **traffic-segmentation forward** можно использовать несколько раз. Все последующие интерфейсы будут добавлены в список участников домена. Используйте форму **no**, чтобы удалить указанный интерфейс из данного списка.

В список участников Traffic Segmentation могут входить различные типы интерфейсов, например, порт и port-channel в одном домене. Если интерфейсы, указанные командой, включают port-channel, все порты-участники данного port-channel будут добавлены в список участников домена.

Если домен продвижения пакетов для интерфейса не указан, то ограничений на продвижение пакетов на указанном порту нет.

Пример

В данном примере показано, как настроить Traffic Segmentation и ограничить домен лавинной рассылки для Ethernet-порта 1/0/1. Установленное ограничение: от Ethernet-порта 1/0/3 до Ethernet- порта 1/0/6.


```
Switch# configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#traffic-segmentation forward interface ethernet 1/0/3-6
Switch(config-if)#
```

95. Команды Virtual LAN (VLAN)

95-1 acceptable-frame

Данная команда используется для настройки допустимых типов кадров на порту. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
acceptable-frame {tagged-only | untagged-only | admit-all}
no acceptable-frame
```

Параметры

tagged-only	Допускаются только тегированные кадры.
untagged-only	Допускаются только нетегированные кадры.
admit-all	Допускаются все кадры.

По умолчанию

Для режима access VLAN mode опцией по умолчанию является **untagged-only**.
Для режима other VLAN mode опцией по умолчанию является **admit-all**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки допустимых типов кадров на порту.

Пример

В данном примере показано, как настроить допустимый тип кадров tagged-only для порта Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# acceptable-frame tagged-only
Switch(config-if)#
```

95-2 ingress-checking

Данная команда используется для включения проверки входящих кадров, получаемых портом. Используйте форму **no** для отключения проверки.

```
ingress-checking
no ingress-checking
```

Параметры

Нет

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для включения проверки входящих кадров, получаемых интерфейсом. При включенной проверке пакет будет отброшен в том случае, если принимающий порт не является членом VLAN, классифицированной для получаемого пакета.

Пример

В данном примере показано, как настроить проверку входящего трафика для включенного порта Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ingress-checking
Switch(config-if)#
```

95-3 mac-vlan

Данная команда используется для создания привязки VLAN на основе MAC-адреса. Используйте форму **no** для удаления привязки VLAN на основе MAC-адреса.

mac-vlan *MAC-ADDRESS* **vlan** *VLAN-ID* [**priority** *COS-VALUE*]
no mac-vlan *MAC-ADDRESS*

Параметры

<i>MAC-ADDRESS</i>	MAC-адрес для привязки.
vlan <i>VLAN-ID</i>	VLAN ID для привязки VLAN на основе MAC-адреса.
priority <i>COS-VALUE</i>	(Опционально) Значение приоритета CoS. Если параметр не указан, то значением CoS по умолчанию является 0.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для создания привязки VLAN на основе MAC-адреса. Классификация привязки будет применена к пакетам, получаемым коммутатором. По умолчанию приоритет для классификации VLAN для нетегированного пакета является MAC-based > Subnet-based > Protocol VLAN.

Пример

В данном примере показано, как создать привязку VLAN ID на основе MAC-адреса для MAC-адреса 00-80-cc-00-00-11.

```
Switch# configure terminal
Switch(config)# mac-vlan 00-80-cc-00-00-11 vlan 101 priority 4
Switch(config)#
```

95-4 protocol-vlan profile

Данная команда используется для создания группы протоколов. Используйте форму **no** для удаления указанной группы протоколов.

```
protocol-vlan profile PROFILE-ID frame-type {ethernet2 | snap | llc} ether-type TYPE-VALUE
no protocol-vlan profile PROFILE-ID
```

Параметры

<i>PROFILE-ID</i>	VLAN ID для привязки Группа протоколов, которую следует добавить или удалить. на основе MAC-адреса.
frame-type	Тип кадров.
ethernet2	Значение для типа кадров Ethernet II.
snap	Значение для типа кадров SNAP.
llc	Значение для типа кадров LLC.
ether-type <i>TYPE-VALUE</i>	Указывает тип. Данное значение должно быть 2-байтным в шестнадцатиричной форме.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду **protocol-vlan profile** в режиме Global Configuration Mode для создания группы протоколов. Затем используйте команду **protocol-vlan profile** в режиме Interface Configuration Mode для настройки классификации VLAN для группы протоколов, получаемых на порту.

Пример

В данном примере показано, как создать VLAN-группу протоколов с идентификатором группы 10, указав, что будет использоваться протокол IPv6 (тип кадров — Ethernet2, значение - 0x86dd).

```
Switch# configure terminal
Switch(config)# protocol-vlan profile 10 frame-type ethernet2 ether-type 0x86dd
Switch(config)#
```

95-5 protocol-vlan profile (Interface)

Данная команда используется для настройки привязки VLAN для группы протоколов на порту. Используйте форму **no** для удаления привязки VLAN на порту.

```
protocol-vlan profile PROFILE-ID vlan VLAN-ID [priority COS-VALUE]
no protocol-vlan profile PROFILE-ID
```

Параметры

<i>PROFILE-ID</i>	Идентификатор группы протоколов, который должен классифицироваться.
vlan <i>VLAN-ID</i>	VLAN ID для protocol VLAN. Для каждой группы привязки может быть указан только один VLAN ID.
priority <i>COS-VALUE</i>	(Опционально) Значение приоритета CoS. Если параметр не указан, то значением CoS по умолчанию является 0.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы указать VLAN для группы протоколов на порту. В результате, пакет, полученный на порту, который соответствует указанной группе протоколов, будет определен в указанную VLAN. VLAN не должна обязательно существовать для настройки команды. Приоритет классификации VLAN для нетегированного пакета является MAC-based > Subnet-based > Protocol VLAN.

Пример

В данном примере показано, как создать привязку VLAN на Ethernet 1/0/1 для классификации пакетов в группе протоколов 10 в VLAN 3000.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# protocol-vlan profile 10 vlan 3000
Switch(config-if)#
```

95-6 show protocol-vlan profile

Данная команда используется для отображения параметров настройки, касающихся protocol VLAN.

show protocol-vlan {profile [*PROFILE-ID* [, | -]] | interface [*INTERFACE-ID* [, | -]]}

Параметры

profile	Группа протоколов.
<i>PROFILE-ID</i>	(Опционально) Группа протоколов, которая должна отображаться.
,	(Опционально) Серия идентификаторов профилей (Profile ID) или разделение идентификаторов профилей от предыдущего диапазона. Перед и после запятой использование пробела недопустимо.
-	(Опционально) Диапазон идентификаторов профилей. Перед дефисом и после дефиса использование пробела недопустимо.
interface	Интерфейсы, которые должны отображаться.
<i>INTERFACE-ID</i>	(Опционально) Порт для отображения настроек классификации protocol VLAN.
,	(Опционально) Диапазон интерфейсов или разделение интерфейсов от предыдущего диапазона. Перед и после запятой использование пробела недопустимо.
-	(Опционально) Диапазон интерфейсов. Перед дефисом и после дефиса использование пробела недопустимо.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду для отображения настроек для классификации VLAN на порту на основе группы протоколов.

Пример

В данном примере показано, как отобразить настройки для классификации VLAN на основе группы протоколов с Ethernet 1/0/1 по 1/0/3.

```
Switch# show protocol-vlan interface ethernet 1/0/1-3
```

Interface	Protocol Group ID	VLAN	Priority
eth1/0/1	1	1	5
eth1/0/2	10	3	0
	11	2001	4
	12	3002	1
eth1/0/3	2	100	6

```
Switch#
```

В данном примере показано, как отобразить настройки профиля группы протоколов.

```
Switch#show protocol-vlan profile
```

Profile ID	Frame-type	Ether-type
1	Ethernet2	0x86DD(IPv6)
2	Ethernet2	0x0800(IP)
3	Ethernet2	0x0806(ARP)

```
Total Entries: 3
```

```
Switch#
```

95-7 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

<i>VLAN-ID</i>	(Опционально) Список VLAN для отображения информации о портах- участниках. Если VLAN не указана, то отображаются все VLAN. Корректный диапазон: от 1 до 4094.
,	(Опционально) Диапазон VLAN или разделение VLAN от предыдущего диапазона. Перед и после запятой использование пробела недопустимо.
-	(Опционально) Диапазон VLAN. Перед дефисом и после дефиса использование пробела недопустимо.
interface <i>INTERFACE-ID</i>	(Опционально) Порт для отображения настроек, касающихся VLAN.
,	(Опционально) Диапазон интерфейсов или разделение интерфейсов от предыдущего диапазона. Перед и после

	запятой использование пробела недопустимо.
-	(Опционально) Диапазон интерфейсов. Перед дефисом и после дефиса использование пробела недопустимо.
mac-vlan	(Опционально) Указывается для отображения информации о VLAN на основе MAC-адресов.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурирования

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения параметров для всех настроенных VLAN или одной VLAN на коммутаторе.

Пример

В данном примере показано, как отобразить все текущие записи VLAN.

```
Switch# show vlan

VLAN 1
  Name : default
  Tagged Member Ports   :
  Untagged Member Ports : 1/0/1-1/0/8

Total Entries : 1

Switch#
```

В данном примере показано, как отобразить информацию о PVID, проверке входящих пакетов и допустимых типах кадров для ethernet 1/0/1-1/0/4.


```

Switch# show vlan interface ethernet 1/0/1-1/0/4

eth1/0/1
VLAN mode          : Trunk
Native VLAN        : 5 (Untagged)
Trunk allowed VLAN : 2,4,5,6
Ingress checking   : Enabled
Acceptable frame type : Admit-all
Dynamic Tagged VLAN : 100

eth1/0/2
VLAN mode          : Access
Access VLAN        : 2
Ingress checking   : Enabled
Acceptable frame type : Untagged-only

eth1/0/3
VLAN mode          : Hybrid
Native VLAN        : 5
Hybrid untagged VLAN : 2,4,5,6
Hybrid tagged VLAN  : 8,9,10
Ingress checking   : Enabled
Acceptable frame type : Admit-All
Dynamic tagged VLAN :
VLAN Precedence    : MAC-VLAN

eth1/0/4
VLAN mode          : Dot1q-tunnel
Access VLAN        : 800
Hybrid untagged VLAN : 200, 600
Ingress checking   : Enabled
Acceptable frame type : Admit-all
VLAN Precedence    : MAC-VLAN

Switch#

```

В данном примере показано, как отобразить все привязки VLAN на основе MAC-адресов.

```

Switch# show vlan mac-vlan

MAC Address          VLAN ID  Priority  Status
-----
00-80-cc-00-00-11   101      4        Active
00-11-22-00-00-05   200      5        Active

Total Entries: 2

Switch#

```

95-8 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

<i>VLAN-ID</i>	Access VLAN интерфейса.
----------------	-------------------------

По умолчанию

По умолчанию access VLAN является VLAN 1.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда вступает в силу, когда интерфейс настроен в режиме доступа (access mode) или режиме dot1q-tunnel mode. VLAN, указанная в качестве access VLAN, не должна обязательно существовать для настройки команды. Может быть указана только одна access VLAN. Следующая команда перезаписывает предыдущую команду.

Пример

В данном примере показано, как настроить ethernet 1/0/1 в режиме доступа (access mode) с access VLAN 1000.

```
Switch# configure terminal  
Switch(config)# interface ethernet 1/0/1  
Switch(config-if)# switchport mode access  
Switch(config-if)# switchport access vlan 1000  
Switch(config-if)#
```

95-9 switchport hybrid allowed vlan

Данная команда используется для указания тегированных или нетегированных VLAN для гибридного порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
switchport hybrid allowed vlan {[add] {tagged | untagged} | remove} VLAN-ID [, | -]  
no switchport hybrid allowed vlan
```

Параметры

add	(Опционально) Порт, который будет добавлен в указанную(-ые) VLAN.
tagged	Указывает порт в качестве тегированного для указанной(-

	ых) VLAN.
untagged	Указывает порт в качестве нетегированного для указанной(-ых) VLAN.
remove	Порт, который будет удален из указанной(-ых) VLAN.
VLAN-ID	Список разрешенных VLAN или список VLAN, который будет добавлен или удален из списка разрешенных VLAN. Если опция не задана, указанный список VLAN перезапишет список разрешенных VLAN.
,	(Опционально) Диапазон VLAN или разделение VLAN от предыдущего диапазона. Перед и после запятой использование пробела недопустимо.
-	(Опционально) Диапазон VLAN. Перед дефисом и после дефиса использование пробела недопустимо.

По умолчанию

По умолчанию гибридный порт является нетегированным членом VLAN 1.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Настраивая команду hybrid VLAN несколько раз с разными VLAN ID порт может стать тегированным или нетегированным членом нескольких VLAN.

Когда разрешенная VLAN указана только как VLAN ID, следующая команда перезапишет предыдущую команду. Если новый нетегированный разрешенный список VLAN перекрывается с текущим списком тегированных разрешенных VLAN, то перекрывающаяся часть будет изменена на нетегированную разрешенную VLAN. С другой стороны, если новый список тегированных разрешенных VLAN перекрывается с текущим списком нетегированных разрешенных VLAN, то перекрывающаяся часть будет изменена на тегированную разрешенную VLAN. Последняя команда вступит в силу. VLAN не должна обязательно существовать для настройки команды.

Пример

В данном примере показано, как настроить ethernet 1/0/1 в качестве тегированного порта VLAN 1000 и нетегированного порта VLAN 2000 и 3000.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode hybrid
Switch(config-if)# switchport hybrid allowed vlan add tagged 1000
Switch(config-if)# switchport hybrid allowed vlan add untagged 2000,3000
Switch(config-if)#
```

95- 10 switchport hybrid native vlan

Данная команда используется для указания native VLAN ID гибридного порта. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
switchport hybrid native vlan VLAN-ID
no switchport hybrid native vlan
```

Параметры

VLAN-ID	Native VLAN гибридного порта.
---------	-------------------------------

По умолчанию

По умолчанию native VLAN гибридного порта является VLAN 1.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

При настройке привязки гибридного порта к его native VLAN используйте команду **switchport hybrid allowed vlan**, чтобы добавить native VLAN в ее разрешенную VLAN. Указанная VLAN не должна обязательно существовать для применения этой команды. Команда вступает в силу, когда интерфейс настроен в гибридном режиме.

Пример

В данном примере показано, как настроить ethernet 1/0/1, чтобы он стал гибридным интерфейсом, и настроить PVID 20.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode hybrid
Switch(config-if)# switchport hybrid allowed vlan add untagged 1000,20
Switch(config-if)# switchport hybrid native vlan 20
Switch(config-if)#
```

95-11 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 | dot1q-tunnel}
no switchport mode
```

Параметры

access	Указывает порт в качестве порта доступа.
hybrid	Указывает порт в качестве гибридного порта.

trunk	Указывает порт в качестве trunk-порта.
dot1q-tunnel	Указывает порт в качестве порта dot1q-tunnel.

По умолчанию

По умолчанию установлена опция **hybrid**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

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.

Примечание: когда режимом switchport mode является **access**, только нетегированные пакеты могут быть перенаправлены через MPLS Virtual Circuit (VC). Чтобы обеспечить возможность перенаправления как тегированных, так и нетегированных пакетов через MPLS VC, настройте режим switchport mode как trunk. **(Только для MI)**

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)#
```

95-12 switchport trunk allowed vlan

Данная команда используется для настройки VLAN, которым разрешено получать и отправлять трафик на указанный интерфейс в тегированном формате. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
switchport trunk allowed vlan {all | [add | remove | except] VLAN-ID [, | -]}
no switchport trunk allowed vlan
```

Параметры

all	VLAN, которые разрешены на интерфейсе.
add	Добавление списка указанных VLAN в список разрешенных VLAN.
remove	Удаление списка указанных VLAN из списка разрешенных VLAN.
except	Указывает, что разрешены все VLAN, за исключением VLAN, находящихся в списке исключений.
<i>VLAN-ID</i>	Список разрешенных VLAN или список VLAN, которые должны быть добавлены в список разрешенных VLAN или удалены из него.
,	(Опционально) Диапазон VLAN или разделение VLAN от предыдущего диапазона. Перед и после запятой использование пробела недопустимо.
-	(Опционально) Диапазон VLAN. Перед дефисом и после дефиса использование пробела недопустимо.

По умолчанию

По умолчанию все VLAN разрешены.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда вступает в силу, только когда интерфейс настроен в режиме trunk mode. Если VLAN разрешена на trunk-порту, то порт станет тегированным членом VLAN. Когда для разрешенной VLAN установлена опция all, то порт будет автоматически добавлен во все VLAN, созданные системой.

Пример

В данном примере показано, как настроить ethernet 1/0/1 в качестве тегированного члена VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 1000
Switch(config-if)#
```

95-13 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

<i>VLAN-ID</i>	Native VLAN для trunk-порта.
tag	Включение режима тегирования (tagging mode) native VLAN.

По умолчанию

По умолчанию задана native VLAN 1, режим нетегированный.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда вступает в силу, только когда интерфейс настроен в режиме trunk mode. Когда native VLAN trunk-порта настроен в тегированном режиме (tagged mode), обычно допустимый тип кадров порта должен быть настроен как “tagged-only”, чтобы принимать только тегированные кадры. Когда trunk- порт работает в нетегированном режиме (untagged mode) для native VLAN, передавая нетегированный пакет для native VLAN и тегированные пакеты для всех остальных VLAN, допустимые типы кадров порта должны быть настроены как “admit-all” для корректной работы.

Указанная VLAN не должна обязательно существовать для настройки команды.

Пример

В данном примере показано, как настроить ethernet 1/0/1 в качестве интерфейса trunk и native VLAN 20.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 20
Switch(config-if)#
```

95-14 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

<i>VLAN-ID</i>	Идентификатор VLAN, которая должны быть добавлена, удалена или настроена. Корректный диапазон VLAN ID: от 1 до 4094. VLAN ID 1 не может быть удален.
,	(Опционально) Диапазон VLAN или разделение VLAN от

	предыдущего диапазона. Перед и после запятой использование пробела недопустимо.
-	(Опционально) Диапазон VLAN. Перед дефисом и после дефиса использование пробела недопустимо.

По умолчанию

VLAN ID 1 существует в системе в качестве VLAN по умолчанию.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду глобальной настройки **vlan** для создания VLAN. Ввод команды **vlan** с VLAN ID влечет вход в режим настройки VLAN (VLAN configuration mode). Ввод VLAN ID существующей VLAN не создает новую VLAN, но разрешает пользователю изменить параметры VLAN для указанной VLAN. Когда пользователь вводит VLAN ID новой VLAN, VLAN будет создана автоматически.

Используйте команду **no vlan** для удаления VLAN. VLAN по умолчанию не может быть удален. 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)#
```

95-15 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для указания имени VLAN. Имя VLAN должно быть уникальным в административном домене.

Пример

В данном примере показано, как настроить имя VLAN «admin-vlan» для VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# name admin-vlan
Switch(config-vlan)#
```

96. Команды Virtual LAN (VLAN) Tunnel

96-1 switchport mode dot1q-tunnel

Данная команда используется для указания внутреннего идентификатора протокола тега (TPID, Tag Protocol Identifier) системы. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

switchport mode dot1q-tunnel

Параметры

Нет

По умолчанию

По умолчанию порт коммутатора функционирует как гибридный порт.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команда используется для настройки интерфейсов физического порта и port-channel.

Порт 802.1Q tunnel выступает в роли UNI-порта сервисной VLAN. Trunk-порт, тегированный как член сервисной VLAN, выступает в роли NNI-порта сервисной VLAN.

802.1Q tunnel может работать на основе порта (Port-Based Tunnel), на основе VLAN (VLAN-Based Tunnel) или на основе потока (Flow-Based Tunnel). В туннеле на основе порта все принятые пакеты отправляются через общую сервисную VLAN. В туннеле на основе VLAN пакеты могут отправляться через разные сервисные VLAN, при этом сервисная VLAN определяется на основе таблицы соответствия VLAN. В туннеле, основанном на потоке, пакеты отправляются через разные сервисные VLAN. Сервисная VLAN определяется согласно правилу соответствия VLAN на основе потока. Ниже указан приоритет (Precedence) для классификации входящих пакетов:

Flow-Based VLAN Tunnel > VLAN-Based Tunnel > Port-Based Tunnel

Для туннеля на основе портов сервисная VLAN задаётся командой **switchport access vlan**, то есть порт будет настроен как нетегированный член сервисной VLAN.

Для туннеля на основе VLAN или туннеля на основе потока порт следует настроить как нетегированный член всех сервисных VLAN, заданных в таблице или профиле соответствия. Нетегированное членство в сервисной VLAN задаётся командой **switchport hybrid allowed vlan**.

Пример

В данном примере показано, как перевести порт в режим dot1q-tunnel mode.

```
Switch# configure terminal
Switch(config)# interface eth1/0/2
Switch(config)# switchport mode dot1q-tunnel
Switch(config)#
```

96-2 dot1q inner ethertype

Данная команда используется для указания внутреннего TPID системы. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

dot1q inner ethertype *VALUE*
no dot1q inner ethertype

Параметры

<i>VALUE</i>	Укажите внутренний TPID системы в шестнадцатеричном виде. Доступный диапазон значений: от 0x1 до 0xFFFF.
--------------	---

По умолчанию

TPID по умолчанию – 0x8100.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить внутренний TPID системы, который определяет был ли добавлен тег C-VID к входящему пакету. Значение внутреннего TPID настраивается для устройства в целом.

Пример

В данном примере показано, как настроить значение внутреннего TPID системы. Настроенное значение – 0x9100.

```
Switch# configure terminal
Switch(config)# dot1q inner ethertype 0x9100
Switch(config)#
```

96-3 dot1q tunneling ethertype

Данная команда используется для указания внешнего TPID сервисной VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

dot1q tunneling ethertype *VALUE*
no dot1q tunneling ethertype

Параметры

<i>VALUE</i>	Укажите внешний TPID сервисной VLAN в шестнадцатеричном виде. Доступный диапазон значений: от 0x1 до 0xFFFF.
--------------	---

По умолчанию

Значение по умолчанию – 0x8100.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Порт 802.1Q tunnel выступает в роли UNI-порта сервисной VLAN. Trunk-порт, тегированный как член сервисной VLAN, выступает в роли NNI-порта сервисной VLAN.

Настройка туннелирования 802.1Q типа Ethernet возможна только на портах, подключенных к сети моста провайдера, которая принимает и передает тегированные кадры сервисной VLAN. Если настроен тип туннеля Ethernet, то указанное значение TPID будет внешним тегом VLAN передаваемых кадров из данного порта. Заданный TPID также используется для идентификации тега сервисной VLAN для принятого кадра на данном порту.

Пример

В данном примере показано, как настроить значение TPID туннелирования 802.1Q на интерфейсе Ethernet 1/0/1. Настроенное значение – 0x88a8.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# dot1q tunneling ethertype 0x88a8
Switch(config-if)#
```

96-4 switchport vlan mapping

Данная команда используется для указания записи VLAN Translation на trunk-порту или записи привязки сервисной VLAN на порту dot1q tunnel. Используйте форму **no**, чтобы удалить запись VLAN Translation или запись привязки сервисной VLAN.

switchport vlan mapping original-vlan ORIGINAL-VLAN [, | -] {[ORIGINAL-INNER-VLAN] resultant-vlan RESULTANT-VLAN[RESULTANT-INNER-VLAN] | dot1q-tunnel DOT1Q-TUNNEL-VLAN} [priority COS-VALUE]
no switchport vlan mapping original-vlan ORIGINAL-VLAN [, | -] [ORIGINAL-INNER-VLAN]

Параметры

<i>ORIGINAL-VLAN</i>	Укажите исходный VLAN ID, соответствующий входящим пакетам, в диапазоне от 1 до 4094.
<i>ORIGINAL-INNER-VLAN</i>	(Опционально) Укажите, чтобы сопоставить исходную внутреннюю (inner) VLAN с внутренним (inner) VID для входящих пакетов на порту в режиме trunk mode. Доступный диапазон значений: от 1 до 4094.
<i>RESULTANT-VLAN</i>	Укажите Translated ID сервисной VLAN в диапазоне от 1 до 4094, чтобы заменить исходную VLAN для соответствующих пакетов.
<i>RESULTANT-INNER-VLAN</i>	(Опционально) Укажите новую внутреннюю (inner) VLAN, чтобы заменить исходную внутреннюю (inner) VLAN на порту в режиме trunk mode.
<i>DOT1Q-TUNNEL-VLAN</i>	Укажите, чтобы добавить ID сервисной VLAN для соответствующих пакетов на порту в режиме dot1q-tunnel mode.
<i>COS-VALUE</i>	(Опционально) Укажите приоритет правила. Если приоритет тега сервисной VLAN не задан, будет использовано значение по умолчанию – 0.
,	(Опционально) Используется для перечисления нескольких VLAN или от деления диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Команду можно применить только на порту или на port-channel, которые установлены в режиме 802.1Q tunnel mode или в режиме trunk mode.

Если указан параметр **dot1q-tunnel**: при соответствии тега C-VLAN входящего пакета указанной исходной VLAN, заданная S-VLAN будет добавлена для пометки пакета с двойным тегом. Укажите диапазон VLAN, которых необходимо преобразовать в единую сеть S-VLAN. Данное правило можно настроить на порту 802.1Q tunnel только в активном режиме.

Если указан параметр *RESULTANT-VLAN*, будет выполнено VLAN Translation. При соответствии тега VLAN входящего пакета указанной исходной VLAN, заданная S-VLAN заменяет исходную VLAN. VLAN Translation – это преобразование «один-к-одному», то есть преобразование нескольких исходных VLAN в одну S-VLAN невозможна. VLAN Translation можно настроить как на порту 802.1Q tunnel, так и на trunk-порту.

(Опционально) Чтобы настроить правило VLAN Translation 2:1, укажите параметр *ORIGINAL-INNER-VLAN*. В данном случае внешний и внутренний теги входящих пакетов соответствуют правилу VLAN Translation.

Внешняя VLAN соответствующего пакета заменяется Translated сервисной VLAN, а исходная внутренняя VLAN не изменяется.

Чтобы настроить правило VLAN Translation 2:2, укажите параметр *RESULTANT-INNER-VLAN*. В данном случае исходная внутренняя VLAN соответствующего пакета будет заменена новой заданной внутренней VLAN.

Обычно VLAN Translation 2:1 и 2:2 конфигурируются на trunk-портах.

Если на trunk-порту настроены записи VLAN Mapping, обработка пакетов осуществляется по-другому. VLAN пакета, прибывшего на порт, преобразуется в новую VLAN. Затем изучение и последующие операции основываются на Translated VLAN. Перед осуществлением передачи исходящего пакета его VLAN вновь преобразуется в исходную VLAN.

При настройке записей VLAN Mapping для преобразования исходной VLAN в S-VLAN нельзя настроить другую запись VLAN Mapping для преобразований других исходных VLAN в S-VLAN или настроить правило VLAN Mapping, объединяющее C-VLAN в S-VLAN, и наоборот.

Если на соответствующем входящем помеченном пакете запись или правило VLAN Mapping не применены, при включенной функции VLAN Mapping Missdrop пакет будет отброшен. Если функция VLAN Mapping Missdrop отключена, для несогласованного пакета будет назначена сервисная VLAN на основе порта.

Пример

В данном примере показано, как настроить записи VLAN Mapping на trunk-порту.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport vlan mapping original-vlan 100 resultant-vlan 1100
Switch(config-if)# switchport vlan mapping original-vlan 200 resultant-vlan 1200
Switch(config-if)#
```

В данном примере показано, как настроить записи VLAN Mapping на порту 802.1Q tunnel.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# switchport vlan mapping original-vlan 600 resultant-vlan 1600
Switch(config-if)# switchport vlan mapping original-vlan 700 dot1q-tunnel 1700
Switch(config-if)# switchport access vlan 1600
Switch(config-if)# switchport hybrid allow vlan add untagged 1700
Switch(config-if)#
```

96-5 dot1q-tunnel insert dot1q-tag

Данная команда используется для вставки тега dot1q VLAN. Используйте форму **no**, чтобы удалить вставку тега dot1q VLAN.

dot1q-tunnel insert dot1q-tag *DOT1Q-VLAN*
no dot1q-tunnel insert dot1q-tag

Параметры

DOT1Q-VLAN

Укажите ID dot1q VLAN для нетегированных пакетов,

полученных на порту dot1q tunnel.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы вставить внутренний тег dot1q VLAN в пакеты, которые были получены на порту 802.1Q tunnel.

Пример

В данном примере показано, как вставить внутренний тег VLAN 10 для интерфейса порта 1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# dot1q-tunnel insert dot1q-tag 10
Switch(config-if)#
```

96-6 vlan mapping miss drop

Данная команда используется для включения функции VLAN Mapping Missdrop для отбрасывания несоответствующих пакетов. Используйте форму **no**, чтобы отключить функцию VLAN Mapping Missdrop.

vlan mapping miss drop
no vlan mapping miss drop

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для интерфейсов физического порта и port-channel, на которых включен режим 802.1Q tunnel mode. При включенной функции VLAN Mapping Missdrop пакеты, исходная VLAN которых не соответствует записям и правилам VLAN Mapping, будут отброшены.

Пример

В данном примере показано, как включить функцию VLAN Mapping Missdrop для интерфейса порта 1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# vlan mapping miss drop
Switch(config-if)#
```

96-7 dot1q-tunnel trust inner-priority

Данная команда используется для установки доверенного приоритета dot1q. Используйте форму **no**, чтобы удалить настройку.

```
dot1q-tunnel trust inner-priority
no dot1q-tunnel trust inner-priority
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы скопировать приоритет тега dot1q VLAN полученных пакетов в тег сервисной VLAN.

Пример

В данном примере показано, как настроить доверенный внутренний приоритет (Trust Inner-Priority) для интерфейса порта 1.


```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# dot1q-tunnel trust inner-priority
Switch(config-if)#
```

96-8 vlan mapping profile

Данная команда используется для создания профиля VLAN Mapping или входа в режим конфигурации профиля VLAN Mapping. Используйте форму **no**, чтобы удалить профиль VLAN Mapping.

vlan mapping profile *ID* [**type** [ethernet] [ip] [ipv6]]

no vlan mapping profile *ID*

Параметры

<i>ID</i>	Укажите ID профиля VLAN Mapping. ID с более низким значением имеет более высокий приоритет. Доступный диапазон значений ID: от 1 до 1000.
type	(Опционально) Укажите типы профиля. Разным профилям соответствуют разные поля. ethernet : профиль может соответствовать полям 2 уровня. ip : профиль может соответствовать полям IP 3 уровня. ipv6 : профиль может соответствовать IPv6-адресам назначения или источника.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Профиль VLAN Mapping может использоваться для обеспечения гибкого и мощного потокового VLAN Translation. Для создания профиля VLAN Mapping укажите тип профиля, чтобы выбрать, какие поля будут соответствовать правилам профиля.

Пример

В данном примере показано, как создать профиль VLAN Mapping, которому будут соответствовать поля Ethernet.

```
Switch# configure terminal
Switch(config)# vlan mapping profile 1 type ethernet
Switch(config-vlan-map)#
```

96-9 vlan mapping rule

Данная команда используется для настройки правил профиля VLAN Mapping. Используйте форму **no**, чтобы удалить ранее настроенные правила.

```
rule [SN] match [src-mac MAC-ADDRESS] [dst-mac MAC-ADDRESS] [priority COS-VALUE] [inner-vid
VLAN-ID] [ether-type VALUE] [src-ip NETWORK-PREFIX] [dst-ip NETWORK-PREFIX] [src-ipv6 IPV6-NETWORK-
PREFIX/PREFIX-LENGTH] [dst-ipv6 IPV6-NETWORK-PREFIX/PREFIX-LENGTH] [dscp VALUE] [src-port VALUE]
[dst-port VALUE] [ip-protocol VALUE] {dot1q-tunnel | translate} outer-vid VLAN-ID [priority COS-VALUE]
[inner-vid VLAN-ID]
no rule SN[- |,]
```

Параметры

SN	(Опционально) Укажите порядковый номер правила VFP. Если номер не указан, SN начинается с 10 с шагом 10. Доступный диапазон значений SN: от 1 до 10000.
src-mac MAC-ADDRESS	(Опционально) Укажите MAC-адрес источника.
dst-mac MAC-ADDRESS	(Опционально) Укажите MAC-адрес назначения.
priority COS-VALUE	(Опционально) Укажите приоритет 802.1p.
inner-vid VLAN-ID	(Опционально) Укажите внутренний (inner) VLAN ID.
ether-type VALUE	(Опционально) Укажите тип Ethernet.
src-ip NETWORK-PREFIX	(Опционально) Укажите IPv4-адрес источника.
dst-ip NETWORK-PREFIX	(Опционально) Укажите IPv4-адрес назначения.
src-ipv6 IPV6-NETWORK-PREFIX/PREFIX-LENGTH	(Опционально) Укажите IPv6-адрес источника.
dst-ipv6 IPV6-NETWORK-PREFIX/PREFIX-LENGTH	(Опционально) Укажите IPv6-адрес назначения.
dscp VALUE	(Опционально) Укажите значение DSCP.
src-port VALUE	(Опционально) Укажите номер TCP-порта/UDP-порта источника.
dst-port VALUE	(Опционально) Укажите номер TCP-порта/UDP-порта назначения.
ip-protocol VALUE	(Опционально) Укажите значение протокола 3 уровня.
dot1q-tunnel	Укажите, чтобы добавить внешний (outer) VLAN ID для соответствующих пакетов.
translate	Укажите, чтобы заменить внешний (outer) VLAN ID для соответствующих пакетов.
outer-vid VLAN-ID	Укажите новый внешний (outer) VLAN ID.
priority COS-VALUE	(Опционально) Укажите приоритет 802.1p в новом внешнем теге (TAG). Если приоритет нового внешнего тега не задан, будет использовано значение по умолчанию – 0.
inner-vid VLAN-ID	Укажите новый внутренний (inner) VLAN ID.

По умолчанию

Нет

Режим ввода команды

VLAN Mapping Profile Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для настройки правил профиля VLAN Mapping. Если профиль применен на интерфейсе, коммутатор сопоставит входящие пакеты в соответствии с правилами профиля. При соответствии пакетов правилу внешний (outer) VID будет добавлен или заменен. (Опционально) Укажите приоритет нового внешнего тега или укажите новый внутренний (inner) VID пакетов.

Порядок соответствия зависит от порядкового номера правила профиля и прекращается при первом совпадении. Если порядковый номер не указан, значение будет назначено автоматически. Порядковый номер начинается с 10 с шагом 10. На одном интерфейсе можно настроить несколько различных типов профилей.

Пример

В данном примере показано, как настроить правила для профиля 1 VLAN Mapping.

```
Switch# configure terminal
Switch(config)# vlan mapping profile 1 type ip
Switch(config-vlan-map)# rule 10 match src-ip 100.1.1.0/24 dot1q-tunnel outer-vid 100
Switch(config-vlan-map)# rule 20 match dst-ip 200.1.1.0/24 dot1q-tunnel outer-vid 200
Switch(config-vlan-map)#
```

96- 10 switchport vlan mapping profile

Данная команда используется для применения правил профиля VLAN Mapping к указанному интерфейсу. Используйте форму **no**, чтобы удалить привязку.

```
switchport vlan mapping profile PROFILE-ID
no switchport vlan mapping profile PROFILE-ID
```

Параметры

<i>PROFILE-ID</i>	(Опционально) Укажите ID профиля VLAN Mapping.
-------------------	--

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы применить профиль VLAN Mapping к указанному физическому порту или port-channel в режиме dot1q-tunnel mode.

Если профиль применен к интерфейсу, коммутатор проверит входящие пакеты в соответствии с правилами профиля. Если пакеты соответствуют правилу, то к ним будет применено действие правила.

Если настроить порт не в соответствии с правилами режима dot1q-tunnel mode, конфигурация профиля VLAN Mapping будет удалена.

Пример

В данном примере показано, как настроить профиль VLAN Mapping и применить его для порта 1 802.1Q tunnel. Пакеты клиентов, поступающие из 100.1.1.0/24, будут добавлены в S-VLAN 100, а пакеты, поступающие на 200.1.1.0/ 24, будут добавлены в S-VLAN 200.

```
Switch# configure terminal
Switch(config)# vlan mapping profile 1 type ip
Switch(config-vlan-map)# rule 10 match src-ip 100.1.1.0/24 dot1q-tunnel outer-vid 100
Switch(config-vlan-map)# rule 20 match dst-ip 200.1.1.0/24 dot1q-tunnel outer-vid 200
Switch(config-vlan-map)# exit
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport vlan mapping profile 1
Switch(config-if)#
```

96-11 show dot1q ethertype

Данная команда используется для отображения настроек TPID.

show dot1q ethertype [*INTERFACE-ID* [- I,]]

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

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить тип Ethernet тега сервисной VLAN.

Пример

В данном примере показано, как отобразить настройки TPID 802.1Q на всех интерфейсах.

```
Switch#show dot1q ethertype
802.1q inner Ethernet Type is 0x8100
eth1/0/1
802.1q tunneling Ethernet Type is 0x88a8
eth1/0/2
802.1q tunneling Ethernet Type is 0x88a8
Switch#
```

96-12 show dot1q-tunnel

Данная команда используется для отображения настроек туннелирования dot1q VLAN на интерфейсах.

show dot1q-tunnel [interface *INTERFACE-ID* [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите интерфейсы, которые необходимо отобразить. Если интерфейсы не указаны, будут отображены все порты 802.1Q tunnel.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить настройки туннелирования 802.1Q на интерфейсах.

Пример

В данном примере показано, как отобразить настройки всех портов 802.1Q tunnel.

```
Switch# show dot1q-tunnel

dot1q Tunnel Interface: eth1/0/1
Trust inner priority      : Enabled
VLAN mapping miss drop   : Disabled
VLAN mapping profiles    : 1, 2, 3

dot1q Tunnel Interface: eth1/0/2
Trust inner priority      : Disabled
VLAN mapping miss drop   : Enabled
Insert dot1q tag         : VLAN 10

Switch#
```

96-13 show vlan mapping

Данная команда используется для отображения настроек VLAN Mapping.

show vlan mapping [interface *INTERFACE-ID* [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите интерфейсы, которые необходимо отобразить. Если интерфейсы не указаны, будут отображены все VLAN Mapping.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить настройки VLAN Mapping.

Пример

В данном примере показано, как отобразить все VLAN Mapping.

```
Switch#show vlan mapping

Interface      Original VLAN  Translated VLAN  Priority  Status
-----
eth1/0/1      1             dot1q-tunnel 10   0        Active
eth1/0/1      2             dot1q-tunnel 11   5        Active
eth1/0/2      10            Translate 100     0        Active
eth1/0/2      20            Translate 200     0        Active
eth1/0/3      30/3          Translate 300     0        Active
eth1/0/3      40/1          Translate 400/2    2        Active

Total entries: 6

Switch#
```

96-14 show vlan mapping profile

Данная команда используется для отображения информации о настроенном профиле VLAN Mapping.

show vlan mapping profile [ID]

Параметры

<i>ID</i>	(Опционально) Укажите ID профиля VLAN Mapping. Если ID не указан, будут отображены все профили VLAN Mapping.
-----------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить настроенный профиль VLAN Mapping.

Пример

В данном примере показано, как отобразить информацию обо всех профилях VLAN Mapping.

```
Switch# show vlan mapping profile
```

```
VLAN mapping profile:1 type:ip
```

```
rule 10 match src-ip 100.1.1.0/24, action dot1q-tunnel outer-vid 100, priority 0
```

```
rule 20 match dst-ip 200.1.1.0/24, action dot1q-tunnel outer-vid 200, priority 1
```

```
rule 30 match src-ip 192.1.1.0/24, action dot1q-tunnel outer-vid 300, priority 0
```

```
Total Entries: 3
```

```
VLAN mapping profile:2 type:ethernet
```

```
rule 10 match src-mac 00-00-00-00-00-01,action translate outer-vid 40, priority 2
```

```
rule 20 match inner-vid 5, action translate outer-vid 10, priority 0
```

```
Total Entries: 2
```

```
Switch#
```


97. Команды Virtual Router Redundancy Protocol (VRRP)

97-1 snmp-server enable traps vrrp

Данная команда используется для включения отправки VRRP trap в SNMP. Используйте форму **no**, чтобы отключить отправку VRRP trap.

```
snmp-server enable traps vrrp [new-master] [auth-fail]
no snmp-server enable traps vrrp [new-master] [auth-fail]
```

Параметры

new-master	(Опционально) Укажите, чтобы настроить отправку trap для нового основного устройства (New Master). Если отправка trap включена, при переходе устройства в режим Master будет выслано trap-сообщение.
auth-fail	(Опционально) Укажите, чтобы настроить отправку trap ошибки аутентификации. Если отправка trap включена и маршрутизатором был получен пакет, ключ аутентификации или тип аутентификации которого конфликтует с ключом аутентификации или типом аутентификации этого маршрутизатора, будет выслано trap-сообщение.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить отправку VRRP trap. Если не указан ни один из параметров, оба типа trap-сообщений включаются или отключаются одновременно.

Пример

В данном примере показано, как включить отправку trap для нового основного устройства (Master) VRRP.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps vrrp new-master
Switch(config)#
```

97-2 vrrp authentication

Данная команда используется для включения аутентификации VRRP и установки пароля на интерфейсе. Используйте форму **no**, чтобы отменить аутентификацию.

vrpp authentication *STRING*
no vrrp authentication

Параметры

<i>STRING</i>	Укажите пароль для аутентификации в текстовом формате. Максимально допустимое количество символов в строке – 8.
---------------	---

По умолчанию

По умолчанию аутентификация отсутствует.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить аутентификацию VRRP на интерфейсе. Аутентификация применяется ко всем виртуальным маршрутизаторам на данном интерфейсе. Устройства в одной VRRP-группе должны иметь один пароль аутентификации.

Пример

В данном примере показано, как настроить аутентификацию VRRP одного интерфейса.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# vrrp authentication test
Switch(config-if)#
```

97-3 vrrp ip

Данная команда используется для создания VRRP-группы на интерфейсе. Используйте форму **no**, чтобы удалить VRRP-группу.

vrpp *VRID* ip *IP-ADDRESS*
no vrrp *VRID*

Параметры

<i>VRID</i>	Укажите идентификатор виртуального маршрутизатора, чтобы идентифицировать группу VRRP. Доступный диапазон значений: от 1 до 255.
<i>IP-ADDRESS</i>	Укажите IP-адрес для созданной группы виртуального маршрутизатора.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы создать виртуальный маршрутизатор и задать для него IP-адрес. Маршрутизаторы одной VRRP-группы должны быть настроены с помощью одного и того же ID и IP-адреса.

Группа виртуальных маршрутизаторов представлена одним ID. IP-адрес виртуального маршрутизатора – это шлюз по умолчанию, настроенный на узлах. IP-адрес может быть как действительным адресом, настроенным на маршрутизаторах, так и неиспользуемым адресом. Если виртуальный адрес совпадает с действительным адресом интерфейса, данный виртуальный маршрутизатор является владельцем IP-адреса.

Один из маршрутизаторов данной группы становится основным устройством (Master), другие маршрутизаторы становятся резервными устройствами (Backup). Основное устройство (Master) отвечает за отправку пакетов на виртуальный маршрутизатор.

Пример

В данном примере показано, как создать VRRP-группу на интерфейсе VLAN 1. Идентификатор виртуального маршрутизатора – 7. IP-адрес виртуального маршрутизатора – 10.1.1.1.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# vrrp 7 ip 10.1.1.1
Switch(config-if)#
```

97-4 vrrp bfd

Данная команда используется для настройки адреса узла BFD (Bidirectional Forwarding Detection) VRRP. Используйте форму **no**, чтобы удалить адрес узла BFD VRRP.

```
vrrp VRID bfd fast-detect peer IP-ADDRESS
no vrrp VRID bfd fast-detect peer IP-ADDRESS
```

Параметры

<i>VRID</i>	Укажите идентификатор виртуального маршрутизатора в диапазоне от 1 до 255.
peer <i>IP-ADDRESS</i>	Укажите IP-адрес узла BFD.

По умолчанию

По умолчанию IP-адрес узла BFD не настроен.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить адрес узла BFD VRRP-группы. Данный IP-адрес должен быть действительным IP-адресом действительного устройства в той же VRRP-группе. Сессия BFD будет создана между данным VRRP-маршрутизатором и его узлом. При завершении сессии VRRP-маршрутизатор в роли резервного устройства (Backup) сразу переходит в режим Master.

Пример

В данном примере показано, как настроить адрес узла BFD на интерфейсе VLAN 1. Настроенный адрес – 10.1.1.2.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# vrrp 1 bfd fast-detect peer 10.1.1.2
Switch(config-if)#
```

97-5 vrrp priority

Данная команда используется для настройки приоритета виртуального маршрутизатора. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
vrrp VRID priority PRIORITY
no vrrp VRID priority
```

Параметры

<i>VRID</i>	Укажите идентификатор виртуального маршрутизатора в диапазоне от 1 до 255.
<i>PRIORITY</i>	Укажите приоритет виртуального маршрутизатора в диапазоне от 1 до 254.

По умолчанию

Значение приоритета по умолчанию – 100.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Основное устройство (Master) VRRP-группы определяется исходя из приоритета. Виртуальный маршрутизатор с наивысшим приоритетом становится основным устройством (Master), другие маршрутизаторы с более низким приоритетом становятся резервными устройствами (Backup) для VRRP-группы. Если значения приоритетов маршрутизаторов равны, сравниваются их IP-адреса – маршрутизатору с наибольшим IP-адресом будет присвоен статус основного устройства (Master).

Маршрутизатор, владеющий IP-адресом VRRP-группы, всегда выступает в роли основного устройства (Master) и имеет самый высокий приоритет – 255.

Пример

В данном примере показано, как настроить приоритет на значение 200.

```
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#vrrp 1 priority 200
Switch(config-if)#
```

97-6 vrrp non-owner-ping

Данная команда позволяет виртуальному маршрутизатору в роли основного устройства (Master) отвечать на эхо-запросы ICMP для IP-адреса, который не принадлежит данному маршрутизатору, но ассоциирован с ним. Используйте форму **no**, чтобы отключить ответ на Ping.

```
vrrp non-owner-ping
no vrrp non-owner-ping
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

В некоторых условиях виртуальный маршрутизатор в роли основного устройства (Master) должен отвечать на эхо-запросы ICMP для IP-адреса, который не принадлежит данному маршрутизатору.

Пример

В данном примере показано, как разрешить всем виртуальным маршрутизаторам отвечать на эхо-запросы ICMP.

```
Switch# configure terminal
Switch(config)# vrrp non-owner-ping
Switch(config)#
```

97-7 vrrp timers advertise

Данная команда используется для настройки интервала между последовательными VRRP- Advertisement, отправленными Master-маршрутизатором. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
vrrp VRID timers advertise INTERVAL
no vrrp VRID timers advertise
```

Параметры

<i>VRID</i>	Укажите идентификатор виртуального маршрутизатора, чтобы идентифицировать группу VRRP. Доступный диапазон значений: от 1 до 255.
<i>INTERVAL</i>	Укажите временной интервал между последовательными VRR-Advertisement, отправленными Master-маршрутизатором. Доступный диапазон значений: от 1 до 255 секунд.

По умолчанию

Интервал по умолчанию – 1 секунда.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Основное устройство (Master) постоянно присылает VRRP-Advertisement для передачи информации о текущем Master-маршрутизаторе. Используйте данную команду, чтобы настроить интервал между пакетами Advertisement и время до того, как другие маршрутизаторы признают Master-маршрутизатор выключенным. Виртуальные маршрутизаторы одной VRRP-группы должны использовать одинаковые значения таймера.

Пример

В данном примере показано, как указать интервал между VRRP-Advertisement для VRRP 7 на интерфейсе VLAN 1. Настроенный интервал – 10 секунд.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# vrrp 7 timers advertise 10
Switch(config-if)#
```

97-8 vrrp preempt

Данная команда позволяет маршрутизатору взять на себя роль основного устройства (Master), если у него более высокий приоритет, чем у текущего устройства (Master). Используйте форму **no**, чтобы вернуться к режиму Non-Preempt Mode.

```
vrrp VRID preempt  
no vrrp VRID preempt
```

Параметры

<i>VRID</i>	Укажите идентификатор виртуального маршрутизатора, чтобы идентифицировать группу VRRP. Доступный диапазон значений: от 1 до 255.
-------------	--

По умолчанию

По умолчанию режим Preempt Mode используется.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

В режиме Preempt Mode маршрутизатор, имеющий более высокий приоритет, чем текущий Master, берет на себя роль основного устройства.

В режиме Non-Preempt Mode замены Master не происходит, если IP-адрес не принадлежит входящему маршрутизатору.

Пример

В данном примере показано, как вытеснить текущий Master-маршрутизатор с более низким приоритетом и настроить новый Master-маршрутизатор для VRRP-группы 7.

```
Switch# configure terminal  
Switch(config)# interface vlan 1  
Switch(config-if)# vrrp 7 preempt  
Switch(config-if)#
```

97-9 vrrp shutdown

Данная команда используется для отключения виртуального маршрутизатора на интерфейсе. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
vrrp VRID shutdown  
no vrrp VRID shutdown
```

Параметры

<i>VRID</i>	Укажите идентификатор виртуального маршрутизатора, чтобы идентифицировать группу VRRP. Доступный диапазон значений: от 1 до 255.
-------------	--

По умолчанию

По умолчанию виртуальный маршрутизатор начинает работу после его создания.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используя данную команду, обратите внимание, что сначала нужно выключить маршрутизаторы, не являющиеся владельцами IP-адреса, затем маршрутизатор, являющийся владельцем.

Пример

В данном примере показано, как отключить один VRRP VRID 1 на интерфейсе VLAN 1, сохранив при этом VRRP VRID 2.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# vrrp 1 shutdown
Switch(config-if)# no vrrp 2 shutdown
Switch(config-if)#
```

97-10 vrrp track critical-ip

Данная команда используется для настройки критического IP-адреса виртуального маршрутизатора. Используйте форму **no**, чтобы удалить критический IP-адрес.

```
vrrp VRID track critical-ip IP-ADDRESS
no vrrp VRID track critical-ip
```

Параметры

<i>VRID</i>	Укажите идентификатор виртуального маршрутизатора, чтобы идентифицировать группу VRRP. Доступный диапазон значений: от 1 до 255.
<i>IP-ADDRESS</i>	Укажите критический IP-адрес.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы задать критический IP-адрес для одного виртуального маршрутизатора. Одна группа VRRP может отслеживать только один критический IP-адрес. Критический IP-адрес выключенного маршрутизатора недоступен.

Пример

В данном примере показано, как настроить критический IP-адрес виртуального маршрутизатора 1 на VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# vrrp 1 track critical-ip 192.168.100.1
Switch(config-if)#
```

98. Команды Virtual Router Redundancy Protocol Version 3 (VRRPv3)

98-1 vrrp address-family

Данная команда используется для создания виртуального VRRP-маршрутизатора и входа в режим Address Family Configuration Mode с использованием IPv4 или IPv6. Используйте форму **no**, чтобы удалить группу.

```
vrrp VRID address-family {ipv4 | ipv6}
no vrrp VRID address-family {ipv4 | ipv6}
```

Параметры

<i>VRID</i>	Укажите идентификатор виртуального маршрутизатора, чтобы идентифицировать группу VRRP. Доступный диапазон значений: от 1 до 255.
<i>ipv4</i>	Укажите, чтобы создать виртуальный маршрутизатор IPv4.
<i>ipv6</i>	Укажите, чтобы создать виртуальный маршрутизатор IPv6.

По умолчанию

Нет

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы создать VRRP-маршрутизатор и войти в режим Address Family Configuration Mode с использованием IPv4 или IPv6.

Пример

В данном примере показано, как создать виртуальный VRRP-маршрутизатор и войти в режим Address Family Configuration Mode с использованием IPv4.

```
Switch#configure terminal
Switch(config)#interface vlan 3
Switch(config-if)#vrrp 1 address-family ipv4
Switch(config-af-vrrp)#
```

98-2 non-owner-ping

Данная команда позволяет виртуальному маршрутизатору в роли основного устройства (Master) отвечать на эхо-запрос ICMP для IPv4-адреса или запрос ND для IPv6-адреса, который не принадлежит данному маршрутизатору, но ассоциирован с ним. Используйте форму **no**, чтобы отключить ответ на Ping.

non-owner-ping
no non-owner-ping

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

VRRP Address Family Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы включить/отключить ответы на эхо-запросы ICMP на виртуальном маршрутизаторе в роли основного устройства (Master) для IPv4-адреса или запрос ND для IPv6-адреса.

Пример

В данном примере показано, как включить функцию Non-Owner-Ping.

```
Switch#configure terminal
Switch(config)#interface vlan 3
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#non-owner-ping
Switch(config-af-vrrp)#
```

98-3 address

Данная команда используется для настройки виртуального адреса IPv4 или IPv6 для одного виртуального маршрутизатора. Используйте форму **no**, чтобы удалить виртуальный адрес.

address {IP-ADDRESS | IPV6 -ADDRESS}
no address {IP-ADDRESS | IPV6 -ADDRESS}

Параметры

<i>IP-ADDRESS</i>	Укажите виртуальный IPv4-адрес виртуального маршрутизатора.
<i>IPV6 -ADDRESS</i>	Укажите виртуальный IPv6-адрес виртуального маршрутизатора.

По умолчанию

Нет

Режим ввода команды

VRRP Address Family Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить виртуальный адрес IPv4 или IPv6 для одного виртуального маршрутизатора. Маршрутизаторы одной VRRP-группы должны быть настроены с помощью одного и того же ID и адреса. IP-адрес может быть как действительным адресом, настроенным на маршрутизаторах, так и неиспользуемым адресом. Если виртуальный адрес совпадает с действительным адресом интерфейса, данный виртуальный маршрутизатор является владельцем IP-адреса.

Пример

В данном примере показано, как настроить виртуальный адрес IPv6 для VRRP-группы.

```
Switch#configure terminal
Switch(config)#interface vlan 3
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#address FE80::2
Switch(config-af-vrrp)#
```

98-4 priority

Данная команда используется для настройки приоритета виртуального маршрутизатора. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

priority *PRIORITY*
no priority

Параметры

<i>PRIORITY</i>	Укажите приоритет виртуального маршрутизатора в диапазоне от 1 до 254.
-----------------	--

По умолчанию

Приоритет по умолчанию – 100.

Режим ввода команды

VRRP Address Family Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Основное устройство (Master) VRRP-группы определяется исходя из приоритета. Виртуальный маршрутизатор с наивысшим приоритетом становится основным устройством (Master), а другие маршрутизаторы с более низким приоритетом становятся резервными устройствами (Backup) для VRRP-группы. Если значения приоритетов маршрутизаторов равны, сравниваются их IP-адреса – маршрутизатору с наибольшим IP-адресом будет присвоен статус основного устройства (Master).

Маршрутизатор, владеющий IP-адресом VRRP-группы, всегда выступает в роли основного устройства (Master) и имеет самый высокий приоритет – 255.

Пример

В данном примере показано, как настроить приоритет на значение 200.

```
Switch#configure terminal
Switch(config)#interface vlan 3
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#priority 200
Switch(config-af-vrrp)#
```

98-5 timers advertise

Данная команда используется для настройки интервала между последовательными VRRP- Advertisement. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

timers advertise *INTERVAL*
no timers advertise

Параметры

<i>INTERVAL</i>	Укажите временной интервал между последовательными VRRP-Advertisement, отправленными Master-маршрутизатором. Доступный диапазон значений: от 1 до 255 секунд.
-----------------	---

По умолчанию

Интервал по умолчанию – 1 секунда.

Режим ввода команды

VRRP Address Family Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Основное устройство (Master) постоянно отправляет VRRP-Advertisement. На виртуальных маршрутизаторах одной VRRP-группы должны быть настроены одинаковые значения таймера.

Пример

В данном примере показано, как указать интервал между VRRP-Advertisement для VRRP 1 на интерфейсе VLAN 3. Настроенный интервал – 10 секунд.

```
Switch#configure terminal
Switch(config)#interface vlan 3
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#timers advertise 10
Switch(config-af-vrrp)#
```

98-6 preempt

Данная команда позволяет маршрутизатору взять на себя роль основного устройства (Master), если у него более высокий приоритет, чем у текущего устройства (Master). Используйте форму **no**, чтобы вернуться к режиму Non-Preempt Mode.

preempt
no preempt

Параметры

Нет

По умолчанию

По умолчанию используется режим Preempt Mode.

Режим ввода команды

VRRP Address Family Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду **no preempt**, чтобы отключить функцию Preempt для сохранения статуса участников VRRP-группы.

Пример

В данном примере показано, как отключить функцию Preempt.

```
Switch#configure terminal
Switch(config)#interface vlan 3
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#no preempt
Switch(config-af-vrrp)#
```

98-7 shutdown

Данная команда используется для отключения виртуального маршрутизатора. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

shutdown
no shutdown

Параметры

Нет

По умолчанию

По умолчанию виртуальный маршрутизатор начинает работу после его создания.

Режим ввода команды

VRRP Address Family Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используя данную команду, обратите внимание, что сначала нужно выключить маршрутизаторы, не являющиеся владельцами IP-адреса, затем маршрутизатор, являющийся владельцем.

Пример

В данном примере показано, как удалить виртуальный маршрутизатор на интерфейсе VLAN 3.

```
Switch#configure terminal
Switch(config)#interface vlan 3
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#shutdown
Switch(config-af-vrrp)#
```

98-8 track critical-ip

Данная команда используется для настройки критического IP-адреса виртуального маршрутизатора. Используйте форму **no**, чтобы удалить критический IP-адрес.

track critical-ip {IP-ADDRESS} [INTERFACE-ID] IPV6-ADDRESS}
no track critical-ip

Параметры

<i>IP-ADDRESS</i>	Задайте критический IP-адрес.
<i>INTERFACE-ID</i>	(Опционально) Укажите интерфейс критического IP-адреса, который необходимо использовать.
<i>IPV6-ADDRESS</i>	Задайте критический IPv6-адрес.

По умолчанию

Нет

Режим ввода команды

VRRP Address Family Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы задать критический IP-адрес для одного виртуального маршрутизатора. Одна группа VRRP может отслеживать только один критический IP-адрес. Критический IP-адрес выключенного маршрутизатора недоступен.

Пример

В данном примере показано, как настроить критический адрес IPv6 виртуального маршрутизатора 1 на VLAN 1.

```
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#track critical-ip vlan 1 FE80::2
Switch(config-af-vrrp)#
```

98-9 show vrrp

Данная команда используется для отображения настроек и статуса VRRP.

```
show vrrp [interface INTERFACE-ID [VRID]] [ipv4 | ipv6]
```

Параметры

<i>INTERFACE-ID</i>	(Опционально) Укажите ID интерфейса.
<i>VRID</i>	(Опционально) Укажите идентификатор виртуального маршрутизатора, чтобы идентифицировать VRRP-группу. Доступный диапазон значений: от 1 до 255.
<i>ipv4</i>	(Опционально) Укажите, чтобы отобразить информацию о виртуальных маршрутизаторах IPv4.
<i>ipv6</i>	(Опционально) Укажите, чтобы отобразить информацию о виртуальных маршрутизаторах IPv6.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить настройки и статус VRRP.

Пример

В данном примере показано, как отобразить статус VRRP для всех интерфейсов.

```
Switch#show vrrp

vlan 3 - Group 1 - Version3 - Address-Family IPv6
  State is Init
  Virtual IP Address is ::
  Virtual MAC Address is 00-00-5E-00-02-01
  Advertisement interval is 1 seconds
  Preemption is enabled
  Priority is 100
  No critical IP address
  Disable non owner ping
  Master Router is ::

Total Entries: 1

Switch#
```

98- 10 show vrrp brief

Данная команда используется для отображения краткой информации о VRRP.

show vrrp brief

Параметры

Нет

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить краткую информацию о VRRP.

Пример

В данном примере показано, как отобразить краткую информацию о VRRP.

```
Switch#show vrrp brief

Interface VRID Ver  AF  Pri Owner Pre State  VRouter IP
-----
vlan 3      1   3 IPv6 100      Y  Init  ::

Total Entries: 1

Switch#
```

99. Команды Voice VLAN

99-1 voice vlan

Данная команда используется для глобального включения функции Voice VLAN и её настройки. Используйте форму **no**, чтобы отключить функцию Voice VLAN.

```
voice vlan VLAN-ID
no voice vlan
```

Параметры

VLAN-ID	Укажите VLAN ID голосовой VLAN в диапазоне от 2 до 4094.
---------	--

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для глобального включения функции Voice VLAN и 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)#
```

99-2 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для настройки времени устаревания для VoIP-устройства и автоматически изученных Member-портов Voice VLAN. Когда последнее VoIP-устройство, подключенное к порту, перестает отправлять трафик и MAC-адрес данного устройства устаревает в FDB, запускается таймер времени устаревания Voice VLAN. По истечении данного времени порт будет удален из Voice VLAN. Если голосовой трафик возобновляется в течение времени устаревания, таймер будет отменен.

Пример

В данном примере показано, как настроить время устаревания Voice VLAN на 30 минут.

```
Switch# configure terminal
Switch(config)# voice vlan aging 30
Switch(config)#
```

99-3 voice vlan enable

Данная команда используется для включения функции Voice VLAN на портах. Используйте форму **no**, чтобы отключить функцию Voice VLAN на портах.

voice vlan enable
no voice vlan enable

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте команду **voice vlan** в режиме Global Configuration Mode и **voice vlan enable** в режиме Interface Configuration Mode, чтобы включить функцию Voice VLAN на портах доступа или гибридных портах.

Пример

В данном примере показано, как включить функцию Voice VLAN на физическом порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# voice vlan enable
Switch(config-if)#
```

99-4 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.
description <i>TEXT</i>	(Опционально) Укажите описание OUI. Максимально допустимое количество символов – 32.

По умолчанию

OUI по умолчанию указаны в следующей таблице:

OUI	Vendor
00:E0:BB	ЗСОМ
00:03:6B	Cisco
00:E0:75	Veritel
00:D0:1E	Pingtel
00:01:E3	Siemens

00:60:B9	NEC/Philips
00:0F:E2	Huawei-3COM
00:09:6E	Avaya

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для добавления уникального идентификатора организации (OUI), определяемого с устройства системы IP-телефонии. OUI используется для идентификации VoIP- трафика с помощью функции Voice VLAN. Если MAC-адреса источника полученных пакетов соответствуют любому из шаблонов OUI, полученные пакеты распознаются как VoIP-пакеты.

OUI, определяемый с устройства системы IP-телефонии, не может совпадать с OUI по умолчанию. OUI по умолчанию не может быть удален.

Пример

В данном примере показано, как добавить OUI для устройства системы IP-телефонии.

```
Switch# configure terminal
Switch(config)# voice vlan mac-address 00-02-03-00-00-00 FF-FF-FF-00-00-00 description User1
Switch(config)#
```

99-5 voice vlan mode

Данная команда используется для включения автоматического изучения порта в качестве Member- порта Voice VLAN. Используйте форму **no**, чтобы отключить автоматическое изучение.

```
voice vlan mode {manual | auto {tag | untag}}
no voice vlan mode
```

Параметры

manual	Укажите, чтобы настроить членство Voice VLAN вручную.
auto	Укажите, чтобы изучить участников Voice VLAN автоматически.
tag	Укажите, чтобы изучить тегированных участников Voice VLAN.
untag	Укажите, чтобы изучить нетегированных участников Voice VLAN.

По умолчанию

Параметры по умолчанию – **untag** или **auto**.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду, чтобы настроить автоматическое изучение Member-портов Voice VLAN или назначить их вручную.

Если автоматическое изучение включено, порт будет автоматически распознан в качестве участника Voice VLAN. В дальнейшем участники будут автоматически удалены согласно времени устаревания. Когда порт работает в автотегируемом режиме (**Auto Tagged Mode**) и фиксирует VoIP-устройство через OUI, он автоматически присоединится к Voice VLAN как тегируемый порт. Если VoIP-устройство отправляет тегируемые пакеты, коммутатор изменит их приоритет. Нетегируемые пакеты отправляются в PVID VLAN порта.

Когда порт работает в автонетегируемом режиме (**Auto Untagged Mode**) и получает информацию о VoIP-устройстве через OUI, он автоматически присоединится к Voice VLAN как нетегируемый порт. Если VoIP-устройство отправляет тегируемые пакеты, коммутатор изменит их приоритет. Нетегируемые 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 тегируемого или нетегируемого Member-порта Voice VLAN.

Пример

В данном примере показано, как настроить автотегируемый 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)#
```

99-6 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

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для маркировки CoS голосовых пакетов, поступающих на порт, на котором включена Voice VLAN. Маркировка CoS позволяет отделить голосовой трафик от трафика данных по качеству обслуживания.

Пример

В данном примере показано, как настроить приоритет Voice VLAN со значением 7.

```
Switch# configure terminal
Switch(config)# voice vlan qos 7
Switch(config)#
```

99-7 show voice vlan

Данная команда используется для отображения настроек Voice VLAN.

show voice vlan [interface [INTERFACE-ID [, | -]]]

show voice vlan {device | lldp-med device} [interface INTERFACE-ID [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально) Укажите, чтобы отобразить информацию о портах Voice VLAN.
,	(Опционально) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
device	Укажите, чтобы отобразить VoIP-устройства, информация о которых была получена через OUI.
lldp-med device	Укажите, чтобы отобразить VoIP-устройства, обнаруженные через LLDP- MED.

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда используется для отображения настроек Voice VLAN.

Пример

В данном примере показано, как отобразить глобальные настройки Voice VLAN.

```
Switch#show voice vlan

Voice VLAN ID      : 3
Voice VLAN CoS     : 5
Aging Time         : 720 minutes
Member Ports       : eth1/0/1-1/0/5
Dynamic Member Ports : eth1/0/1-1/0/3

Voice VLAN CUI     :

OUI Address          Mask                Description
-----
00-01-E3-00-00-00   FF-FF-FF-00-00-00   Siemens
00-02-03-00-00-00   FF-FF-FF-00-00-00   User1
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

Total OUI: 9

Switch#
```

В данном примере показано, как отобразить информацию о портах Voice VLAN.

```
Switch#show voice vlan interface ethernet 1/0/6-10

Interface      State      Mode
-----
eth1/0/6       Enabled    Manual
eth1/0/7       Enabled    Manual
eth1/0/8       Enabled    Manual
eth1/0/9       Enabled    Manual
eth1/0/10      Disabled   Auto/Untag

Switch#
```

В данном примере показано, как отобразить распознанные VoIP-устройства на Ethernet-портах 1/0/1- 1/0/2.

```
Switch#show voice vlan device interface ethernet 1/0/1-2
```

Interface	Voice Device	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#
```

100. Команды Web-аутентификации

100-1 web-auth enable

Данная команда используется для включения функции Web-аутентификации на порту. Используйте форму **no**, чтобы отключить функцию Web-аутентификации.

```
web-auth enable
no web-auth enable
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для аутентификации узлов, подключенных к порту, через Web-браузер.

Пример

В данном примере показано, как включить функцию Web-аутентификации на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# web-auth enable
Switch(config-if)#
```

100-2 web-auth page-element

Данная команда используется для настройки элементов страницы Web-аутентификации. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
web-auth page-element {page-title STRING | login-window-title STRING | username-title STRING |
password-title STRING | logout-window-title STRING | copyright-line LINE-NUMBER titleSTRING}
no web-auth page-element {page-title | login-window-title | username-title | password-title |
logout-window-title | copyright-line}
```

Параметры

page-title *STRING*

Укажите заголовок страницы Web-аутентификации.

	Максимально допустимое количество символов – 128.
login-window-title <i>STRING</i>	Укажите заголовок окна для ввода логина/пароля страницы Web- аутентификации. Максимально допустимое количество символов – 64.
username-title <i>STRING</i>	Укажите название поля для ввода имени пользователя на странице Web- аутентификации. Максимально допустимое количество символов – 32.
password-title <i>STRING</i>	Укажите название поля для ввода пароля на странице Web- аутентификации. Максимально допустимое количество символов – 32.
logout-window-title <i>STRING</i>	Укажите заголовок окна выхода из системы (Logout) на странице Web- аутентификации. Максимально допустимое количество символов – 64.
copyright-line <i>LINE-NUMBER title</i> <i>STRING</i>	Укажите информацию об авторских правах построчно на страницах Web- аутентификации. Максимально допустимое количество строк – 5. Максимально допустимое количество символов для каждой строки – 128.

По умолчанию

Заголовок страницы по умолчанию не установлен.

Заголовок окна для ввода логина/пароля по умолчанию – «Authentication Login».

Название поля для ввода имени пользователя по умолчанию – «User Name».

Название поля для ввода пароля по умолчанию – «Password».

Заголовок окна выхода из системы (Logout) по умолчанию – «Logout From The Network».

Информация об авторских правах по умолчанию не указана.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Элементы страницы Web-аутентификации могут быть настроены от имени администратора. Существуют две страницы Web-аутентификации: (1) страница входа и (2) страница выхода. Введите имя пользователя и пароль на странице входа. Используйте кнопку **Logout**, чтобы выйти из сети.

Пример

В данном примере показано, как изменить информацию об авторских правах в двух строках нижней части страницы аутентификации:

Строка 1: Copyright @ 2015 All Rights

Reserved
Строка 2: Site: <http://support.website.com>

```
Switch# configure terminal
Switch(config)# web-auth page-element copyright-line 1 title Copyright © 2015 All Rights Reserved
Switch(config)# web-auth page-element copyright-line 2 title Site: http://support.website.com
Switch(config)#
```

100-3 web-auth success redirect-path

Данная команда используется для настройки URL, на который клиент будет по умолчанию переадресован после успешной аутентификации. Используйте форму **no**, чтобы удалить указанный URL.

web-auth success redirect-path *STRING*
no web-auth success redirect-path

Параметры

<i>STRING</i>	Укажите URL, на который клиент будет по умолчанию переадресован после успешной аутентификации. Если URL не указан, будет отображена страница выхода Web-аутентификации. Максимально допустимое количество символов переадресации – 128.
---------------	---

По умолчанию

По умолчанию отображается страница выхода Web-аутентификации.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для указания Web-страницы, которую необходимо отобразить узлам, прошедшим Web-аутентификацию.

Пример

В данном примере показано, как настроить путь переадресации, который будет использован по умолчанию после прохождения Web-аутентификации. Настроенный путь – <http://www.website.com>.

```
Switch# configure terminal
Switch(config)# web-auth success redirect-path http://www.website.com
Switch(config)#
```

1004 web-auth system-auth-control

Данная команда используется для глобального включения функции Web-аутентификации на коммутаторе. Используйте форму **no**, чтобы отключить функцию Web-аутентификации глобально на коммутаторе.

web-auth system-auth-control

no web-auth system-auth-control

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Включите функцию Web-аутентификации, чтобы получить доступ к сети Интернет через коммутатор. Коммутатор может выступать как в роли сервера аутентификации, выполняя аутентификацию на основе локальной базы данных, так и в роли клиента RADIUS, выполняя процесс аутентификации по протоколу RADIUS с помощью удаленного сервера RADIUS. В процессе аутентификации используется протокол HTTP или HTTPS.

Пример

В данном примере показано, как включить функцию Web-аутентификации на коммутаторе глобально.

```
Switch# configure terminal
Switch(config)# web-auth system-auth-control
Switch(config)#
```

100-5 web-auth virtual-ip

Данная команда используется для настройки виртуального IP-адреса Web-аутентификации, который используется для приема запросов аутентификации от узла. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

```
web-auth virtual-ip {ipv4 IP-ADDRESS | ipv6 IPV6-ADDRESS | url STRING}
no web-auth virtual-ip {ipv4 | ipv6 | url}
```

Параметры

ipv4 <i>IP-ADDRESS</i>	Укажите виртуальный IPv4-адрес Web-аутентификации.
ipv6 <i>IPV6-ADDRESS</i>	Укажите виртуальный IPv6-адрес Web-аутентификации.
url <i>STRING</i>	Укажите FQDN URL для Web-аутентификации. Максимально допустимое количество символов – 128.

По умолчанию

Нет

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Виртуальный IP-адрес является характеристикой функции Web-аутентификации на коммутаторе. Все процессы Web-аутентификации взаимодействуют с данным IP-адресом. Однако из-за того, что виртуальный IP-адрес не отвечает ни на один пакет ICMP или запрос ARP, настройка виртуального IP-адреса в той же подсети, что и IP-адреса интерфейса коммутатора или подсети узла недопустима. В противном случае, функция Web-аутентификация будет работать некорректно.

Перед использованием указанного URL необходимо настроить виртуальный IP-адрес. Чтобы получить виртуальный IP-адрес, используйте FQDN URL, который хранится на DNS-сервере. Полученный IP-адрес должен соответствовать виртуальному IP-адресу, настроенному с помощью команды. Если IPv4 или IPv6-адрес не настроен, Web-аутентификация невозможна.

Пример

В данном примере показано, как настроить виртуальный IPv4 и FQDN URL для Web-аутентификации. Настроенный IPv4-адрес – 1.1.1.1. Настроенный FQDN URL – www.website4.co.

```
Switch# configure terminal
Switch(config)# web-auth virtual-ip ipv4 1.1.1.1
Switch(config)# web-auth virtual-ip url www.website4.co
Switch(config)#
```

В данном примере показано, как настроить виртуальный IPv6 и FQDN URL для Web-аутентификации. Настроенный IPv6-адрес – 2000::2. Настроенный FQDN URL – www.website6.co.

```
Switch# configure terminal
Switch(config)# web-auth virtual-ip ipv6 2000::2
Switch(config)# web-auth virtual-ip url www.website6.co
Switch(config)#
```

100-6 snmp-server enable traps web-auth

Данная команда используется для включения отправки SNMP-уведомлений для Web-аутентификации. Используйте форму **no**, чтобы отключить отставку SNMP-уведомлений.

```
snmp-server enable traps web-auth
no snmp-server enable traps web-auth
```

Параметры

Нет

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Нет

Пример

В данном примере показано, как включить отправку SNMP-уведомлений для Web-аутентификации.

```
Switch# configure terminal
Switch(config)# snmp server enable traps web-auth
Switch(config)#
```


101. Команды Weighted Random Early Detection(WRED)

101-1 random-detect

Данная команда используется для включения функции WRED. Используйте форму **no**, чтобы отключить функцию WRED.

```
random-detect COS-VALUE [profile ID]
no random-detect COS-VALUE
```

Параметры

<i>COS-VALUE</i>	Укажите очереди CoS, для которых необходимо включить функцию WRED. Доступный диапазон значений: от 0 до 7.
<i>profile ID</i>	(Опционально) Укажите профиль WRED, который необходимо применить. Если профиль не указан, будет использовано пороговое значение по умолчанию.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

При получении пакета текущий средний размер очереди рассчитывается аппаратно.

$$avg_Qsize = current_Qsize + \frac{old_avg_Qsize - current_Qsize}{2^{weight}}$$

Если текущий средний размер очереди меньше минимального порогового значения, поступающий пакет помещается в очередь. Если текущая длина очереди находится между минимальным и максимальным пороговыми значениями очереди, пакет будет либо отброшен, либо будет помещен в очередь в зависимости от вероятности отбрасывания пакета, которая рассчитывается по следующей формуле:

$$DropProbability = \frac{avg_Qsize - MinThreshold}{MaxThreshold - MinThreshold} * MaxDropRate$$

Если средний размер очереди превышает максимальное пороговое значение, будут отброшены все пакеты. Если указанный профиль не существует, будет использовано пороговое значение по умолчанию.

Пример

В данном примере показано, как включить функцию WRED для очереди 5 на интерфейсе Ethernet 1/0/1 и применить профиль 10 WRED.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# random-detect 5 profile 10
Switch(config-if)#
```

101-2 random-detect exponential-weight

Данная команда используется для настройки Exponential Weight Factor WRED для расчета среднего размера очереди. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

random-detect exponential-weight *COS-VALUE* **exponent** *VALUE*
no random-detect exponential-weight *COS-VALUE*

Параметры

<i>COS-VALUE</i>	Укажите очереди CoS, на которых необходимо установить экспоненту. Доступный диапазон значений: от 0 до 7.
exponent <i>VALUE</i>	Укажите значение экспоненты в диапазоне от 0 до 15.

По умолчанию

Exponential weight factor по умолчанию – 9.

Режим ввода команды

Interface Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда используется для настройки Exponential Weight Factor WRED для расчета среднего размера очереди.

Пример

В данном примере показано, как настроить значение экспоненты для очереди 5 на интерфейсе Ethernet 1/0/1. Настроенное значение – 10.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# random-detect exponential-weight 5 exponent 10
Switch(config-if)#
```

101-3 random-detect profile

Данная команда используется для настройки профиля WRED. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

random-detect profile *ID* [**green** | **yellow** | **red**] **min-threshold** *VALUE* **max-threshold** *VALUE* **max-drop-rate** *VALUE*
no random-detect profile *ID*

Параметры

<i>ID</i>	Укажите ID профиля WRED, который необходимо установить.
green	(Опционально) Укажите параметры отбрасывания WRED, которые необходимо установить для зеленых пакетов.
yellow	(Опционально) Укажите параметры отбрасывания WRED, которые необходимо установить для желтых пакетов.
red	(Опционально) Укажите параметры отбрасывания WRED, которые необходимо установить для красных пакетов.
min-threshold <i>VALUE</i>	Укажите минимальное количество ячеек в очереди, после достижения которого пакеты будут отброшены при помощи WRED.
max-threshold <i>VALUE</i>	Укажите максимальное количество ячеек в очереди, после достижения которого все пакеты, предназначенные для данной очереди, будут отброшены при помощи WRED.
max-drop-rate <i>VALUE</i>	Укажите вероятность сброса, в случае если средний размер очереди достигнет максимального порога. Если значение равно нулю, пакет не будет отброшен или отмечен для ECN.

По умолчанию

Значение параметра **min-threshold** по умолчанию – 20.

Значение параметра **max-threshold** по умолчанию – 80.

Значение параметра **max-drop-rate** по умолчанию – 0.

Режим ввода команды

Global Configuration Mode

Уровень команды по умолчанию

Уровень 12

Использование команды

Различные типы пакетов могут быть поставлены в очередь в разных «Bucket Lists», для которых могут быть заданы различные пороговые значения.

Пример

В данном примере показано, как настроить параметры отбрасывания WRED для пакетов всех типов и цветов в профиле 10.

```
Switch# configure terminal
Switch(config)# random-detect profile 10 min-threshold 30 max-threshold 50 max-drop-rate 10
Switch(config)#
```

101-4 show queueing random-detect

Данная команда используется для отображения настроек WRED на указанном интерфейсе.

show queueing random-detect [**interface** *INTERFACE-ID* [, | -]]

Параметры

interface <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

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить настройки WRED. Если ID интерфейса не указан, будут отображены настройки WRED для всех портов системы.

Пример

В данном примере показано, как отобразить настройки WRED и состояние очереди CoS на интерфейсе Ethernet 1/0/1.

```
Switch#show queueing random-detect interface ethernet 1/0/1

Current WRED configuration:

eth1/0/1
CoS  WRED State  Exp-weight-constant  Profile  ECN State
----  -
0    Disabled    9                    1        Disabled
1    Disabled    9                    1        Disabled
2    Enabled     9                    1        Enabled
3    Disabled    9                    1        Disabled
4    Disabled    9                    1        Disabled
5    Disabled    9                    1        Disabled
6    Disabled    9                    1        Disabled
7    Disabled    9                    1        Disabled

Switch#
```

101-5 show random-detect profile

Данная команда используется для отображения настроек профиля WRED.

show random-detect profile [profile ID]

Параметры

profile ID	(Опционально) Укажите ID профиля WRED, который необходимо отобразить. Если профиль не указан, будут отображены настройки всех профилей WRED.
-------------------	--

По умолчанию

Нет

Режим ввода команды

User/Privileged EXEC Mode
Любой режим конфигурации

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить настройки профиля WRED.

Пример

В данном примере показано, как отобразить настройки WRED профиля 1.

```
Switch#show random-detect profile 1
```

```
WRED Profile 1
```

Packet Type	Min-Threshold	Max-Threshold	Max-Drop-Rate
TCP-GREEN	20	80	1
TCP-YELLOW	20	80	5
TCP-RED	20	80	8
NON-TCP-GREEN	20	80	10
NON-TCP-YELLOW	20	80	10
NON-TCP-RED	20	80	10

```
Switch#
```

Приложение А. Восстановление пароля (Password Recovery)

В данной главе представлен процесс сброса паролей на коммутаторах T-KOM серии ТГК-313-24.

Необходимо аутентифицировать любого пользователя, который пытается получить доступ к сети. Основным методом аутентификации пользователей с соответствующими правами является локальная авторизация с помощью имени пользователя (Username) и пароля (Password). В случаях, когда пароли забыты или утеряны, администратору сети необходимо сбросить эти пароли. В данной главе приведена подробная информация о том, как выполнить сброс с помощью функции восстановления пароля.

Ниже представлена информация об использовании функции Password Recovery на коммутаторе для восстановления паролей.

Для сброса пароля выполните следующее:

- В целях безопасности для функции восстановления пароля требуется физический доступ пользователя к устройству. Поэтому данная функция применима только при наличии прямого подключения к консольному порту устройства. Пользователю необходимо подключиться с помощью программы-эмулятора терминала на ПК к консольному порту коммутатора.
- Включите питание коммутатора. После 100% загрузки **UART init** пользователю в течение 2 секунд необходимо нажать горячую клавишу **[^] (Shift+6)** для того, чтобы войти в режим восстановления пароля (Password Recovery Mode). При входе в данный режим все порты будут отключены.

```

Boot Procedure                               V1.00.001
-----
Power On Self Test ..... 100 %

MAC Address   : F0-7D-68-34-00-10
H/W Version   : A1

Please Wait, Loading 1.00.001 Runtime Image ..... 100 %
UART init ..... 100 %

Password Recovery Mode

Switch(reset-config)#
    
```

no enable password	Данная команда используется для удаления всех паролей любого уровня учетных записей.
no login password	Данная команда используется для удаления методов локальной авторизации.
no username	Данная команда используется для удаления всех локальных пользовательских учетных записей.
password-recovery	Данная команда используется для инициирования процесса по восстановлению пароля.
reload	Данная команда используется для сохранения и

	перезагрузки коммутатора.
reload clear running- config	Данная команда используется для сброса текущей конфигурации и восстановления настроек по умолчанию с дальнейшей перезагрузкой коммутатора.
show running-config	Данная команда используется для отображения текущей конфигурации.
show username	Данная команда используется для отображения информации о локальных пользовательских учетных записей.

Приложение Б. Записи системного журнала

В таблице ниже перечислены все записи и их соответствующие значения, появляющиеся в системном журнале коммутатора.

802.1X

Описание записей журнала	Уровень
<p>Описание события: ошибка аутентификации 802.1X.</p> <p>Сообщение в журнале: 802.1X authentication fail [due to <reason>] from (Username: <username>, <interface-id>, MAC: <mac-address>) Описание параметров:</p> <p>reason: причина ошибки аутентификации.</p> <p>username: пользователь, проходящий аутентификацию.</p> <p>interface-id: имя интерфейса.</p> <p>macaddr: MAC-адрес аутентифицированного устройства.</p>	Критический
<p>Описание события: успешная аутентификация 802.1X.</p> <p>Сообщение в журнале: 802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>) Описание параметров:</p> <p>username: пользователь, проходящий аутентификацию.</p> <p>interface-id: имя интерфейса.</p> <p>macaddr: MAC-адрес аутентифицированного устройства.</p>	Информационный

AAA

Описание записей журнала	Уровень
<p>Описание события: глобальное включение/отключение AAA.</p> <p>Сообщение в журнале: AAA is <status>.</p> <p>Описание параметров:</p> <p>status: функция AAA включена или отключена.</p>	Информационный
<p>Описание события: успешный вход.</p> <p>Сообщение в журнале: Successful login through <exec-type> from <client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>).</p> <p>Описание параметров:</p> <p>exec-type: типы EXEC: Console, Telnet, SSH, Web, Web(SSL).</p> <p>client-ip: IP-адрес клиента, доступный для IP-протокола.</p> <p>aaa-method: метод аутентификации: none (аутентификация отсутствует), local (использование локальной базы), server (использование сервера).</p> <p>server-ip: IP-адрес AAA-сервера, если методом аутентификации является удаленный сервер.</p> <p>username: имя пользователя аутентификации.</p>	Информационный
<p>Описание события: ошибка входа.</p> <p>Сообщение в журнале: Login failed through <exec-type> from</p>	Предупреждение

<p><client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>). Описание параметров: exec-type: типы EXEC: Console, Telnet, SSH, Web, Web(SSL). client-ip: IP-адрес клиента, доступный для IP-протокола. aaa-method: метод аутентификации: none (аутентификация отсутствует), local (использование локальной базы), server (использование сервера). server-ip: IP-адрес AAA-сервера, если методом аутентификации является удаленный сервер. username: имя пользователя аутентификации.</p>	
<p>Описание события: ошибка входа из-за тайм-аута или неверной конфигурации AAA-сервера. Сообщение в журнале: Login failed through <exec-type> from <client-ip> due to AAA server <server-ip> timeout (Username: <username>). Описание параметров: exec-type: типы EXEC: Console, Telnet, SSH, Web, Web (SSL). client-ip: IP-адрес клиента, доступный для IP-протокола. server-ip: IP-адрес AAA-сервера, если методом аутентификации является удаленный сервер. username: имя пользователя аутентификации.</p>	Предупреждение
<p>Описание события: успешное включение привилегий. Сообщение в журнале: Successful enable privilege through <exec-type> from <client- ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>). Описание параметров: exec-type: типы EXEC: Console, Telnet, SSH, Web, Web (SSL). client-ip: IP-адрес клиента, доступный для IP-протокола. aaa-method: метод аутентификации: none (аутентификация отсутствует), local (использование локальной базы), server (использование сервера). server-ip: IP-адрес AAA-сервера, если методом аутентификации является удаленный сервер. username: имя пользователя аутентификации.</p>	Информационный
<p>Описание события: ошибка включения привилегий. Сообщение в журнале: Enable privilege failed through <exec-type> from <client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>). Описание параметров: exec-type: типы EXEC: Console, Telnet, SSH, Web, Web (SSL). client-ip: IP-адрес клиента, доступный для IP-протокола. aaa-method: метод аутентификации: none (аутентификация отсутствует), local (использование локальной базы), server (использование сервера). server-ip: IP-адрес AAA-сервера, если методом аутентификации является удаленный сервер. username: имя пользователя аутентификации.</p>	Предупреждение
<p>Описание события: Удаленный сервер не отвечает на запрос аутентификации с применением пароля.</p>	Предупреждение

Сообщение в журнале: Enable privilege failed through <exec-type> from <client-ip> due to AAA server <server-ip> timeout (Username: <username>).	
<p>Описание параметров:</p> <p>exec-type: типы EXEC: Console, Telnet, SSH, Web, Web (SSL).</p> <p>client-ip: IP-адрес клиента, доступный для IP-протокола.</p> <p>server-ip: IP-адрес AAA-сервера, если методом аутентификации является удаленный сервер.</p> <p>username: имя пользователя аутентификации.</p>	
<p>Описание события: RADIUS назначил атрибуты допустимого VLAN ID. Сообщение в журнале: RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>)</p> <p>Описание параметров:</p> <p>server-ip: IP-адрес RADIUS-сервера.</p> <p>vid: назначенный VLAN ID, авторизованный RADIUS-сервером. interface-id: номер порта аутентифицированного клиента. username: имя пользователя аутентификации.</p>	Информационный
<p>Описание события: RADIUS назначил атрибуты</p> <p>Описание события: RADIUS назначил атрибуты допустимой полосы пропускания. Сообщение в журнале: RADIUS server <server-ip> assigned <direction> bandwidth: <threshold> to port <interface -id> (Username: <username>)</p> <p>Описание параметров:</p> <p>server-ip: IP-адрес RADIUS-сервера.</p> <p>direction: направление полосы пропускания: ingress (входящая) или egress (исходящая).</p> <p>threshold: назначенный порог полосы пропускания, авторизованный RADIUS- сервером.</p> <p>interface-id: номер порта аутентифицированного клиента.</p> <p>username: имя пользователя аутентификации.</p>	Информационный
<p>Описание события: RADIUS назначил атрибуты допустимого приоритета. Сообщение в журнале: RADIUS server <server-ip> assigned 802.1p default priority: <priority> to port <interface -id> (Username: <username>)</p> <p>Описание параметров:</p> <p>server-ip: IP-адрес RADIUS-сервера.</p> <p>priority: Назначенный авторитет, авторизованный RADIUS-сервером. interface-id: Номер порта аутентифицированного клиента.</p> <p>username: Имя пользователя аутентификации.</p>	Информационный
<p>Описание события: RADIUS назначил ACL Script, который не может быть применен в системе из-за недостаточности ресурса.</p> <p>Сообщение в журнале: RADIUS server <server-ip> assigns <username> ACL failure at port <interface -id> (<acl-script>)</p> <p>Описание параметров:</p> <p>server-ip: IP-адрес RADIUS-сервера. username: имя пользователя аутентификации.</p> <p>interface-id: номер порта аутентифицированного клиента.</p>	Предупреждение

acl-script: назначенный ACL Script, авторизованный RADIUS-сервером.

ARP

Описание записей журнала	Уровень
<p>Описание события: добровольный ARP-запрос (Gratuitous ARP) обнаружил, что другой узел уже использует данный IP-адрес.</p> <p>Сообщение в журнале: Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:] portNum>, Interface: <ipif_name>).</p> <p>Описание параметров:</p> <p>ipaddr: заданный IP-адрес, который используется другим узлом. macaddr: заданный MAC-адрес, который используется другим узлом. unitID: ID модуля в стеке. Значение должно быть целым числом.</p> <p>portNum: номер логического порта устройства. Значение должно быть целым числом.</p> <p>ipif_name: имя интерфейса коммутатора, из-за IP-адреса которого возник конфликт.</p>	Предупреждение

Auto-save

Описание записей журнала	Уровень
<p>Описание события: информация о настройках DDP сохраняется автоматически. Сообщение в журнале: CONFIG-6-DDPSAVECONFIG: [Unit <unitID>,] Configuration automatically saved to flash due to configuring from DDP(Username: <username>, IP: <ipaddr>)</p> <p>Описание параметров:</p> <p>Unit: Unit ID.</p> <p>username: имя текущего пользователя. ipaddr: IP-адрес клиента.</p>	Информационный

BPDU Protection

Описание записей журнала	Уровень
<p>Описание события: атака BPDU.</p> <p>Сообщение в журнале: <interface-id> enter STP BPDU under protection state (mode: <mode>)</p> <p>Описание параметров:</p> <p>interface-id: интерфейс, на котором обнаружена атака STP BPDU. mode: режим защиты BPDU интерфейса. Возможные режимы: drop (отбрасывание), block (блокировка) или shutdown (отключение).</p>	Информационный
<p>Описание события: атака BPDU устранена.</p> <p>Сообщение в журнале: <interface-id> recover from BPDU under</p>	Информационный

protection state. Описание параметров:
interface-id: интерфейс, на котором обнаружена атака STP BPDU.

CFM

Описание записей журнала	Уровень
<p>Описание события: обнаружен кросс-коннект. Сообщение в журнале: CFM cross-connect. VLAN:<vlanid>, Local (MD Level:<mdlevel>, Interface:<interface-id>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)</p> <p>Описание параметров: vlanid: идентификатор VLAN MEP. mdlevel: уровень MD MEP. interface-id: номер интерфейса MEP. mepdirection: возможные параметры направления MEP: inward или outward. mepid: MEPID, значение которого равно нулю, неизвестен. macaddr: MAC-адрес MEP, значение которого состоит из всех нулей, неизвестен. Note: в режиме CFM hardware информация об удаленных MEP (mepid и macaddr) неизвестна.</p>	Критический
<p>Описание события: обнаружена ошибка CFM CCM. Сообщение в журнале: CFM error ccm. MD Level:<mdlevel>, VLAN:<vlanid>, Local (Interface:<interface-id>, Direction:<mepdirection>) Remote (MEPID:<mepid>, MAC:<macaddr>)</p> <p>Описание параметров: vlanid: идентификатор VLAN MEP. mdlevel: уровень MD MEP. interface-id: номер интерфейса MEP. mepdirection: возможные параметры направления MEP: inward или outward. mepid: MEPID, значение которого равно нулю, неизвестен. macaddr: MAC-адрес MEP, значение которого состоит из всех нулей, неизвестен. Note: в режиме CFM hardware информация об удаленных MEP (mepid и macaddr) неизвестна.</p>	Предупреждение
<p>Описание события: не удается получить пакет CCM удаленной MEP. Сообщение в журнале: CFM remote down. MD Level:<mdlevel>, VLAN:<vlanid>, Local (Interface:<interface-id>, Direction:<mepdirection>)</p> <p>Описание параметров: vlanid: идентификатор VLAN MEP. mdlevel: уровень MD MEP. interface-id: номер интерфейса MEP. mepdirection: возможные параметры направления MEP: inward или outward. mepid: значение MEP ID. macaddr: MAC-адрес MEP.</p>	Предупреждение
<p>Описание события: сообщение об ошибке MAC удаленной MEP. Сообщение в журнале: CFM remote MAC error. MD Level:<mdlevel>, VLAN:<vlanid>, Local (Interface:<interface-id>, Direction:<mepdirection>) Описание параметров:</p>	Предупреждение

vlanid: идентификатор VLAN MEP. mdlevel: уровень MD MEP.
 interface-id: номер интерфейса MEP.
 mepdirection: возможные параметры направления MEP:
 inward или outward. mepid: значение MEP ID.
 macaddr: MAC-адрес MEP.

Описание события: удаленная MEP обнаружила дефекты CFM. Информационный
 Сообщение в журнале: CFM remote detects a defect. MD
 Level:<mdlevel>, VLAN:<vlanid>, Local (Interface:<interface-id>,
 Direction:<mepdirection>) Описание параметров:
 vlanid: идентификатор VLAN MEP. mdlevel: уровень MD MEP.
 interface-id: номер интерфейса MEP.
 mepdirection: возможные параметры направления MEP:
 inward или outward. mepid: значение MEP ID.
 macaddr: MAC-адрес MEP.

Расширение CFM

Описание записей журнала	Уровень
<p>Описание события: обнаружено состояние AIS. Сообщение в журнале: AIS condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local (Interface:<interface-id>, Direction:<mepdirection>, MEPID:<mepid>) Описание параметров: vlanid: идентификатор VLAN MEP. mdlevel: уровень MD MEP. interface-id: номер интерфейса MEP. mepdirection: направление MEP: inward или outward. mepid: значение MEPID.</p>	Уверомление
<p>Описание события: состояние AIS устранено. Сообщение в журнале: AIS condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local (Interface:<interface-id>, Direction:<mepdirection>, MEPID:<mepid>) Описание параметров: vlanid: идентификатор VLAN MEP. mdlevel: уровень MD MEP. interface-id: номер интерфейса MEP. mepdirection: направление MEP: inward или outward. mepid: значение MEPID.</p>	Уверомление
<p>Описание события: обнаружено состояние LCK. Сообщение в журнале: LCK condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local (Interface:<interface-id>, Direction:<mepdirection>, MEPID:<mepid>) Описание параметров: vlanid: идентификатор VLAN MEP. mdlevel: уровень MD MEP. interface-id: номер интерфейса MEP. mepdirection: направление MEP: inward или outward. mepid: значение MEPID.</p>	Уверомление
<p>Описание события: состояние LCK устранено. Сообщение в журнале: LCK condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local (Interface:<interface-id>, Direction:<mepdirection>, MEPID:<mepid>)</p>	Уверомление

Direction:<mepdirection>, MEPID:<mepid>
 Описание параметров:
 vlanid: идентификатор VLAN MEP. mdlevel: уровень MD MEP.
 interface-id: номер интерфейса MEP.
 mepdirection: направление MEP: inward или outward. mepid:
 значение MEPID.

Конфигурация/ПО

Описание записей журнала	Уровень
<p>Описание события: ПО обновлено успешно. Сообщение в журнале: [Unit <unitID>,] Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Описание параметров: unitID: Unit ID. session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента. serverIP: IP-адрес сервера pathFile: путь и имя файла на сервере</p>	Информационный
<p>Описание события: не удалось обновить ПО. Сообщение в журнале: [Unit <unitID>,] Firmware upgraded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Описание параметров: unitID: Unit ID. session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента. serverIP: IP-адрес сервера pathFile: путь и имя файла на сервере.</p>	Предупреждение
<p>Описание события: ПО успешно выгружено. Сообщение в журнале: [Unit <unitID>,]Firmware uploaded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Описание параметров: unitID: Unit ID. session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента. serverIP: IP-адрес сервера pathFile: путь и имя файла на сервере.</p>	Информационный
<p>Описание события: не удалось выгрузить ПО. Сообщение в журнале: [Unit <unitID>,] Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Описание параметров: unitID: Unit ID. session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента.</p>	<serverIP>, File Name: <pathFile>) Описание параметров: unitID: Unit ID. session: сессия пользователя.

macaddr: MAC-адрес клиента. serverIP: IP-адрес сервера
pathFile: путь и имя файла на сервере.

Описание события: конфигурация успешно загружена.
Сообщение в журнале: [Unit <unitID>,]Configuration downloaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Описание параметров:
unitID: Unit ID.
session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента.
macaddr: MAC-адрес клиента. serverIP: IP-адрес сервера
pathFile: путь и имя файла на сервере.

Описание события: не удалось загрузить конфигурацию.
Сообщение в журнале: [Unit <unitID>,]Configuration downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Описание параметров:
unitID: Unit ID.
session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента.
macaddr: MAC-адрес клиента. serverIP: IP-адрес сервера
pathFile: путь и имя файла на сервере.

Описание события: конфигурация успешно выгружена.
Сообщение в журнале: [Unit <unitID>] Configuration uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Описание параметров:
unitID: Unit ID.
session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента.
macaddr: MAC-адрес клиента. serverIP: IP-адрес сервера
pathFile: путь и имя файла на сервере.

Описание события: не удалось выгрузить конфигурацию.
Сообщение в журнале: [Unit <unitID>] Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP:

Предупреждение

Информационный

Информационный

Предупреждение

Предупреждение

username: имя текущего пользователя. ipaddr: IP-адрес клиента.
macaddr: MAC-адрес клиента. serverIP: IP-адрес сервера
pathFile: путь и имя файла на сервере.

<p>Описание события: не удалось загрузить файлы неизвестного типа. Сообщение в журнале: [Unit <unitID>] Downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Описание параметров: unitID: Unit ID. session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента. serverIP: IP-адрес сервера pathFile: путь и имя файла на сервере.</p>	Предупреждение
--	----------------

DAD

Описание записей журнала	Уровень
<p>Описание события: Событие о дублированном адресе во время процесса DAD будет добавлено в журнал, после того как DUT получит сообщение Neighbor Solicitation (NS). Сообщение в журнале: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Solicitation Messages.</p> <p>Описание параметров: ipv6address: IPv6-адрес сообщений Neighbor Solicitation. interface-id: ID интерфейса порта.</p>	Предупреждение
<p>Описание события: Событие о дублированном адресе во время процесса DAD будет добавлено в журнал, после того как DUT получит сообщение Neighbor Advertisement (NA). Сообщение в журнале: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Advertisement Messages.</p> <p>Описание параметров: ipv6address: IPv6-адрес сообщений Neighbor Advertisement. interface-id: ID интерфейса порта.</p>	Предупреждение

DDM

Описание записей журнала	Уровень
<p>Описание события: какой-либо из параметров SFP превысил порог warning (предупреждение). Сообщение в журнале: Optical transceiver <interface-id> <component> <high-low> warning threshold exceeded.</p> <p>Описание параметров: interface-id: ID интерфейса порта. component: типы порога DDM: temperature (температура), supply voltage (напряжение питание), bias current (ток смещения), TX power/RX power (исходящая/входящая мощность). high-low: верхний или нижний порог.</p>	Предупреждение
<p>Описание события: какой-либо из параметров SFP превысил порог alarm (тревога). Сообщение в журнале: Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded.</p>	Критический

Описание параметров:

interface-id: ID интерфейса порта.

component: типы порога DDM: temperature (температура), supply voltage (напряжение питание), bias current (ток смещения), TX power/RX power (исходящая/входящая мощность).

high-low: верхний или нижний порог.

Описание события: какой-либо из параметров SFP вернулся к нормальному состоянию после превышения порога warning. Предупреждение

Сообщение в журнале: Optical transceiver <interface-id> <component> back to normal.

Описание параметров:

interface-id: ID интерфейса порта.

component: типы порога DDM: temperature (температура), supply voltage (напряжение питание), bias current (ток смещения), TX power/RX power (исходящая/входящая мощность).

DHCPv6 Client

Описание записей журнала	Уровень
<p>Описание события: состояние DHCPv6-клиента на указанном интерфейсе изменено администратором.</p> <p>Сообщение в журнале: DHCPv6 client on interface <ipif-name> changed state to [enabled disabled].</p> <p>Описание параметров: <ipif-name>: имя интерфейса DHCPv6-клиента.</p>	Информационный
<p>Описание события: DHCPv6-клиент получил IPv6-адрес от сервера DHCPv6. Сообщение в журнале: DHCPv6 client obtains an ipv6 address <ipv6address> on interface <ipif-name>.</p> <p>Описание параметров: ipv6address: IPv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса DHCPv6-клиента.</p>	Информационный
<p>Описание события: IPv6-адрес, полученный от сервера DHCPv6, обновляется. Сообщение в журнале: The IPv6 address <ipv6address> on interface <ipif-name> starts renewing.</p> <p>Описание параметров: ipv6address: IPv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса DHCPv6-клиента.</p>	Информационный
<p>Описание события: IPv6-адрес, полученный от сервера DHCPv6, успешно обновлен.</p> <p>Сообщение в журнале: The IPv6 address <ipv6address> on interface <ipif-name> renews success.</p> <p>Описание параметров: ipv6address: IPv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса DHCPv6-клиента.</p>	Информационный
<p>Описание события: выполняется повторная привязка IPv6-адреса, полученного от сервера DHCPv6.</p>	Информационный

<p>Сообщение в журнале: The IPv6 address <ipv6address> on interface <ipif-name> starts rebinding.</p> <p>Описание параметров: ipv6address: IPv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса DHCPv6-клиента.</p>	
<p>Описание события: повторная привязка IPv6-адреса, полученного от сервера DHCPv6, выполнена успешно.</p> <p>Сообщение в журнале: The IPv6 address <ipv6address> on interface <ipif-name> rebinds success.</p> <p>Описание параметров: ipv6address: IPv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса DHCPv6-клиента.</p>	Информационный
<p>Описание события: IPv6-адрес, полученный от сервера DHCPv6, удален. Сообщение в журнале: The IPv6 address <ipv6address> on interface <ipif-name> was deleted.</p> <p>Описание параметров: ipv6address: IPv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса DHCPv6-клиента.</p>	Информационный
<p>Описание события: состояние DHCPv6-клиента PD на указанном интерфейсе изменено администратором.</p> <p>Сообщение в журнале: DHCPv6 client PD on interface <intf-name> changed state to <enabled disabled></p> <p>Описание параметров: intf-name: имя интерфейса DHCPv6-клиента PD.</p>	Информационный
<p>Описание события: DHCPv6-клиент PD получил IPv6-префикс от делегирующего маршрутизатора.</p> <p>Сообщение в журнале: DHCPv6 client PD obtains an ipv6 prefix <ipv6networkaddr> on interface <intf-name></p> <p>Описание параметров: ipv6networkaddr: IPv6-префикс, полученный от делегирующего маршрутизатора. ipif-name: имя интерфейса DHCPv6-клиента PD.</p>	Информационный
<p>Описание события: IPv6-префикс, полученный от делегирующего маршрутизатора, обновляется.</p> <p>Сообщение в журнале: The IPv6 prefix <ipv6networkaddr> on interface <intf-name> starts renewing.</p> <p>Описание параметров: ipv6networkaddr: IPv6-префикс, полученный от делегирующего маршрутизатора. ipif-name: имя интерфейса DHCPv6-клиента PD.</p>	Информационный
<p>Описание события: IPv6-префикс, полученный от делегирующего маршрутизатора, успешно обновлен.</p> <p>Сообщение в журнале: The IPv6 prefix <ipv6networkaddr> on interface <intf-name> renews success.</p> <p>Описание параметров: ipv6networkaddr: IPv6-префикс, полученный от делегирующего маршрутизатора. ipif-name: имя интерфейса DHCPv6-клиента PD</p>	Информационный
<p>Описание события: выполняется повторная привязка IPv6-</p>	Информационный

префикса, полученного от сервера DHCPv6.
 Сообщение в журнале: The IPv6 address <ipv6address> on interface <ipif-name> starts rebinding.
 Описание параметров:
 ipv6networkaddr: IPv6-префикс, полученный от делегирующего маршрутизатора. ipif-name: имя интерфейса DHCPv6-клиента PD.

Описание события: повторная привязка IPv6-префикса, полученного от делегирующего маршрутизатора, выполнена успешно. Информационный
 Сообщение в журнале: The IPv6 prefix <ipv6networkaddr> on interface <intf-name> rebinds success.
 Описание параметров:
 ipv6networkaddr: IPv6-префикс, полученный от делегирующего маршрутизатора. ipif-name: имя интерфейса DHCPv6-клиента PD.

Описание события: IPv6-префикс, полученный от делегирующего маршрутизатора, удален. Информационный
 Сообщение в журнале: The IPv6 prefix <ipv6networkaddr> on interface <intf-name> was deleted.
 Описание параметров:
 ipv6networkaddr: IPv6-префикс, полученный от делегирующего маршрутизатора. ipif-name: имя интерфейса DHCPv6-клиента PD.

DHCPv6 Relay

Описание записей журнала	Уровень
Описание события: состояние функции DHCPv6 relay на указанном интерфейсе изменено администратором. Сообщение в журнале: DHCPv6 relay on interface <ipif-name> changed state to [enabled disabled] Описание параметров: <ipif-name>: имя интерфейса DHCPv6 relay agent.	Информационный

DHCPv6 Server

Описание записей журнала	Уровень
Описание события: используется адрес пула сервера DHCPv6. Сообщение в журнале: The address of the DHCPv6 Server pool <pool-name> is used up. Описание параметров: <pool-name>: имя пула сервера DHCPv6.	Информационный
Описание события: количество назначенных IPv6-адресов достигло 4096. Сообщение в журнале: The number of allocated ipv6 addresses of the DHCPv6 Server pool is equal to 4096.	Информационный

DoS Prevention

Описание записей журнала	Уровень
<p>Описание события: обнаружена DoS-атака.</p> <p>Сообщение в журнале: <dos-type> is dropped from (IP: <ip-address> Port <interface- id>).</p> <p>Описание параметров:</p> <p>dos-type: тип DoS-атаки.</p> <p>ip-address: IP-адрес.</p> <p>interface-id: имя интерфейса.</p>	Уведомление

DULD

Описание записей журнала	Уровень
<p>Описание события: на порту обнаружена потеря связи в одном направлении. Сообщение в журнале: DULD <INTERFACE-ID> is detected as unidirectional link. Описание параметров:</p> <p>INTERFACE-ID: имя интерфейса.</p>	Предупреждение

Dynamic ARP Inspection

Описание записей журнала	Уровень
<p>Описание события: обнаружен запрещенный ARP-пакет.</p> <p>Сообщение в журнале: Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>).</p> <p>Описание параметров:</p> <p>type: тип ARP-пакета: ARP-запрос (Request) или ARP-ответ (Response). ip-address: IP-адрес.</p> <p>macaddr: MAC-адрес. vlanid: VLAN ID</p> <p>interface-id: имя интерфейса.</p>	Предупреждение
<p>Описание события: обнаружен разрешенный ARP-пакет.</p> <p>Сообщение в журнале: Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>).</p> <p>Описание параметров:</p> <p>type: тип ARP-пакета: ARP-запрос (Request) или ARP-ответ (Response). ip-address: IP-адрес.</p> <p>macaddr: MAC-адрес. vlanid: VLAN ID</p> <p>interface-id: имя интерфейса.</p>	Информационный

ERPS

Описание записей журнала	Уровень
<p>Описание события: произошло событие Manual Switch.</p> <p>Сообщение в журнале: "Manual Switch is issued on node (MAC: <macaddr>, instance <InstanceID>)"</p> <p>Описание параметров:</p>	Предупреждение

macaddr: MAC-адрес. InstanceID: ID экземпляра.	
Описание события: обнаружено отсутствие сигнала. Сообщение в журнале: "Signal fail detected on node (MAC: <macaddr>, instance <InstanceID>)" Описание параметров: macaddr: MAC-адрес. InstanceID: ID экземпляра.	Предупреждение
Описание события: отсутствие сигнала устранено. Сообщение в журнале: "Signal fail cleared on node (MAC: <macaddr>, instance <InstanceID>)" Описание параметров: macaddr: MAC-адрес. InstanceID: ID экземпляра.	Предупреждение
Описание события: произошло событие Force Switch. Сообщение в журнале: "Force Switch is issued on node (MAC: <macaddr>, instance <InstanceID>)" Описание параметров: macaddr: MAC-адрес. InstanceID: ID экземпляра.	Предупреждение
Описание события: выполнена отмена события. Сообщение в журнале: "Clear command is issued on node (MAC: <macaddr>, instance <InstanceID>)" Описание параметров: macaddr: MAC-адрес. InstanceID: ID экземпляра.	Предупреждение
Описание события: конфликт RPL owner. Сообщение в журнале: "RPL owner conflicted on the node (MAC: <macaddr>, instance <InstanceID>)" Описание параметров: macaddr: MAC-адрес. InstanceID: ID экземпляра.	Предупреждение

Ethernet OAM

Описание записей журнала	Уровень
Описание события: событие Ethernet OAM dying gasp (удаленно). Сообщение в журнале: OAM dying gasp event received (Port<interface-id>) Описание параметров: interface-id: имя интерфейса.	Предупреждение
Описание события: событие Ethernet OAM dying gasp (локально). Сообщение в журнале: Device encountered an OAM dying gasp event.	Предупреждение
Описание события: событие Ethernet OAM critical (удаленно). Сообщение в журнале: OAM critical event received (Port<interface-id>) Описание параметров: interface-id: имя интерфейса.	Предупреждение
Описание события: событие Ethernet OAM critical (локально). Сообщение в журнале: Device encountered an OAM critical event (Port<interface-id>, <condition>) Описание параметров: interface-id: имя интерфейса. condition: строка, отображающая состояние генерируемых критических событий соединения, например, функция OAM отключена (OAM disable), порт отключен (Port shutdown),	Предупреждение

соединение на порту прервано (Port link down), перегруженность пакетами (Packet overload).	
Описание события: событие Error symbol period (удаленно). Сообщение в журнале: Errored symbol period event received (Port <interface-id>) Описание параметров: interface-id: имя интерфейса.	Предупреждение
Описание события: событие Error frame. Сообщение в журнале: Errored frame event received (Port <interface-id>) Описание параметров: interface-id: имя интерфейса.	Предупреждение
Описание события: событие Error frame period. Сообщение в журнале: Errored frame period event received(Port <interface-id>) Описание параметров: interface-id: имя интерфейса.	Предупреждение
Описание события: событие Error frame seconds summary. Сообщение в журнале: Errored frame seconds summary event received (Port <interface-id>) Описание параметров: interface-id: имя интерфейса.	Предупреждение
Описание события: запуск опции Remote loopback. Сообщение в журнале: OAM Remote loopback started (Port <interface-id>) Описание параметров: interface-id: имя интерфейса.	Предупреждение
Описание события: остановка опции remote loopback. Сообщение в журнале: OAM Remote loopback stopped (Port <interface-id>) Описание параметров: interface-id: имя интерфейса.	Предупреждение

Interface

Описание записей журнала	Уровень
Описание события: соединение на порту установлено. Сообщение в журнале: Port <portNum> link up, <link state> Описание параметров: portNum: номер логического порта устройства. Значение должно быть целым числом. link state: например: 100Mbps FULL duplex (100 Мбит/с, режим полного дуплекса).	Информационный
Описание события: соединение на порту прервано. Сообщение в журнале: Port <portNum> link down portNum: номер логического порта устройства. Значение должно быть целым числом.	Информационный

IP Directed Broadcast

Описание записей журнала	Уровень
Описание события: скорость направленных	Информационный

широковещательных рассылок превысила 50 пакетов в секунду в определенной подсети.

Сообщение в журнале: IP Directed Broadcast packet rate is high on subnet. [(IP: %s)] Описание параметров:

IP: адрес назначения (destination) широковещательной рассылки.

Описание события: скорость направленных широковещательных рассылок превысила 100 пакетов в секунду.

Информационный

Сообщение в журнале: IP Directed Broadcast rate is high.

IPSG

Описание записей журнала

Уровень

Описание события: ошибка создания записи DHCP Snooping в таблице IPSG из-за отсутствия ресурсов аппаратных правил.

Предупреждение

Сообщение в журнале: Failed to set IPSG entry due to no hardware rule resource. (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Interface <INTERFACE-ID>)

Описание параметров: ip-address: IP-адрес. macaddr: MAC-адрес. vlanid: VLAN ID

interface-id: имя интерфейса.

LACP

Описание записей журнала

Уровень

Описание события: группа агрегирования (Link Aggregation) включена. Сообщение в журнале: Link Aggregation Group <group_id> link up.

Информационный

Описание параметров:

group_id: ID включенной группы агрегирования.

Описание события: группа агрегирования (Link Aggregation) отключена. Сообщение в журнале: Link Aggregation Group <group_id> link down.

Информационный

Описание параметров:

group_id: ID включенной группы агрегирования.

Описание события: Member-порт присоединился к группе агрегирования. Сообщение в журнале: <ifname> attach to Link Aggregation Group <group_id>. Описание параметров:

Информационный

Ifname: имя интерфейса порта, который был присоединен к группе агрегирования. group_id: ID группы агрегирования, к которой был присоединен порт.

Описание события: Member-порт покинул группу агрегирования.

Информационный

Сообщение в журнале: <ifname> detach from Link Aggregation Group <group_id>. Описание параметров:

Ifname: имя интерфейса порта, который покинул группу агрегирования. group_id: ID группы агрегирования, которую

покинул порт.

LBD

Описание записей журнала	Уровень
<p>Описание события: обнаружена петля в режиме Port-Based. Сообщение в журнале: IfInfo LBD loop occurred.</p> <p>Описание параметров: IfInfo: информация об интерфейсе.</p>	Критический
<p>Описание события: порт вернулся в исходное состояние в режиме Port-Based. Сообщение в журнале: IfInfo LBD loop recovered.</p> <p>Описание параметров: IfInfo: информация об интерфейсе.</p>	Критический
<p>Описание события: обнаружена петля в режиме VLAN-Based. Сообщение в журнале: IfInfo VID <vlanID> LBD loop occurred.</p> <p>Описание параметров: IfInfo: информация об интерфейсе. vlanID: номер VLAN ID.</p>	Критический
<p>Описание события: порт вернулся в исходное состояние в режиме VLAN-Based. Сообщение в журнале: IfInfo LBD loop recovered.</p> <p>Описание параметров: IfInfo: информация об интерфейсе. vlanID: номер VLAN ID.</p>	Критический
<p>Описание события: число VLAN, на которых была обнаружена петля, превысило указанное число. Сообщение в журнале: Loop VLAN numbers overflow.</p>	Критический

LLDP-MED

Описание записей журнала	Уровень
<p>Описание события: обнаружено изменение топологии LLDP-MED. Сообщение в журнале: LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) Описание параметров: portNum: номер порта. chassisType: список подтипов ID шасси:</p> <ol style="list-style-type: none"> 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 	Уведомление

-
- 6. interfaceName(6)
 - 7. local(7)
 - chassisID: ID шасси.
 - portType: список подтипов ID порта:

- 1. interfaceAlias(1)
- 2. portComponent(2)
- 3. macAddress(3)
- 4. networkAddress(4)
- 5. interfaceName(5)
- 6. agentCircuitId(6)
- 7. local(7)

portID: ID порта.

deviceClass: тип устройства LLDP-MED.

Описание события: обнаружен конфликт типа устройства LLDP-MED. Сообщение в журнале: Conflict LLDP-MED device type detected (on port

Уведомление

<portNum>, chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)

Описание параметров: portNum: номер порта.

chassisType: список подтипов ID шасси:

chassis

- 1. Component(1)
- 2. interfaceAlias(2)
- 3. portComponent(3)
- 4. macAddress(4)
- 5. networkAddress(5)
- 6. netwinterfaceName(6)
- 7. local(7)

chassisID: ID шасси.

portType: список подтипов ID порта:

- 1. interfaceAlias(1)
- 2. portComponent(2)
- 3. macAddress(3)
- 4. networkAddress(4)
- 5. interfaceName(5)
- 6. agentCircuitId(6)
- 7. local(7)

portID: ID порта.

deviceClass: тип устройства LLDP-MED.orkAddress(5)

Описание события: обнаружен несовместимый набор TLV LLDP-MED. Сообщение в журнале: Incompatible LLDP-MED TLV set detected (on port

Уведомление

<portNum>, chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)

Описание параметров: portNum: номер порта.

chassisType: список подтипов ID шасси:

chassis

1. Component(1)
2. interfaceAlias(2)
3. portComponent(3)
4. macAddress(4)
5. networkAddress(5)
6. interfaceName(6)
7. local(7)

chassisID: ID шасси.

portType: список подтипов ID порта:

1. interfaceAlias(1)
2. portComponent(2)
3. macAddress(3)
4. networkAddress(4)
5. interfaceName(5)
6. agentCircuitId(6)
7. local(7)

portID: ID порта.

deviceClass: тип устройства LLDP-MED.

Login/Logout

Описание записей журнала	Уровень
<p>Описание события: успешный вход через консоль.</p> <p>Сообщение в журнале: [Unit <unitID>,] Successful login through Console (Username: <username>) Описание параметров: unitID: Unit ID. username: имя текущего пользователя.</p>	Информационный
<p>Описание события: не удалось выполнить вход через консоль.</p> <p>Сообщение в журнале: [Unit <unitID>,] Login failed through Console (Username: <username>) Описание параметров: unitID: Unit ID. username: имя текущего пользователя.</p>	Предупреждение
<p>Описание события: время сессии в консоли истекло.</p> <p>Сообщение в журнале: [Unit <unitID>,] Console session timed out (Username: <username>) Описание параметров: unitID: Unit ID. username: имя текущего пользователя.</p>	Информационный
<p>Описание события: выполнен выход через консоль.</p> <p>Сообщение в журнале: [Unit <unitID>,] Logout through Console (Username: <username>) Описание параметров: unitID: Unit ID.</p>	Информационный

username: имя текущего пользователя.	
Описание события: успешный вход через Telnet. Сообщение в журнале: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Информационный
Описание события: не удалось выполнить вход через Telnet. Сообщение в журнале: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Информационный
Описание события: время сессии Telnet истекло. Сообщение в журнале: Telnet session timed out (Username: <username>, IP: <ipaddr>) Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Информационный
Описание события: выполнен выход через Telnet. Сообщение в журнале: Logout through Telnet (Username: <username>, IP: <ipaddr>) Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Информационный
Описание события: успешный вход через SSH. Сообщение в журнале: Successful login through SSH (Username: <username>, IP: <ipaddr>) Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Информационный
Описание события: не удалось выполнить вход через SSH. Сообщение в журнале: Login failed through SSH (Username: <username>, IP: <ipaddr>) Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Критический
Описание события: время сессии SSH истекло. Сообщение в журнале: SSH session timed out (Username: <username>, IP: <ipaddr>) Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес	Информационный

клиента.	
Описание события: выполнен выход через SSH.	Информационный
Сообщение в журнале: Logout through SSH (Username: <username>, IP: <ipaddr>) Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	

MAC

Описание записей журнала	Уровень
Описание события: хост успешно прошел аутентификацию на основе MAC. Сообщение в журнале: MAC-based Access Control host login success (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Описание параметров: mac-address: MAC-адрес хоста. interface-id: интерфейс, на котором аутентифицирован хост. vlan-id: ID VLAN, в которой находится хост.	Информационный
Описание события: время аутентификации хоста истекло. Сообщение в журнале: MAC-based Access Control host aged out (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Описание параметров: mac-address: MAC-адрес хоста. interface-id: интерфейс, на котором аутентифицирован хост. vlan-id: ID VLAN, в которой находится хост.	Информационный
Описание события: хост не прошел аутентификацию. Сообщение в журнале: MAC-based Access Control host login fail (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Описание параметров: mac-address: MAC-адрес хоста. interface-id: интерфейс, на котором аутентифицирован хост. vlan-id: ID VLAN, в которой находится хост.	Критический
Описание события: количество авторизованных пользователей на устройстве достигло максимального значения. Сообщение в журнале: MAC-based Access Control enters stop learning state.	Предупреждение
Описание события: количество авторизованных пользователей на устройстве вернулось к значению ниже максимального за заданный интервал времени. Сообщение в журнале: MAC-based Access Control recovers from stop learning state.	Предупреждение
Описание события: количество авторизованных пользователей на интерфейсе достигло максимального значения. Сообщение в журнале: <interface-id> enters MAC-based Access Control stop learning state Описание параметров: interface-id: интерфейс, на котором аутентифицирован хост.	Предупреждение

<p>Описание события: количество авторизованных пользователей на интерфейсе вернулось к значению ниже максимального за заданный интервал времени.</p> <p>Сообщение в журнале: <interface-id> recovers from MAC-based Access Control stop learning state.</p> <p>Описание параметров: interface-id: интерфейс, на котором аутентифицирован хост.</p>	Предупреждение
--	----------------

MSTP Debug Enhancement

Описание записей журнала	Уровень
<p>Описание события: топология изменилась.</p> <p>Сообщение в журнале: Topology changed [[[Instance:<InstanceID>], <portNum> ,MAC: <macaddr>]] Описание параметров: InstanceID: ID экземпляра. portNum: ID порта. macaddr: MAC-адрес.</p>	Уведомление
<p>Описание события: новый корневой мост.</p> <p>Сообщение в журнале: [CIST CIST Regional MSTI Regional] New Root bridge selected([Instance: <InstanceID>],MAC: <macaddr>, Priority :<value>) Описание параметров: InstanceID: ID экземпляра. macaddr: MAC-адрес. value: значение приоритета</p>	Информационный
<p>Описание события: Spanning Tree Protocol включен.</p> <p>Сообщение в журнале: Spanning Tree Protocol is enabled</p>	Информационный
<p>Описание события: Spanning Tree Protocol отключен.</p> <p>Сообщение в журнале: Spanning Tree Protocol is disabled</p>	Информационный
<p>Описание события: новый корневой порт.</p> <p>Сообщение в журнале: New root port selected [[[Instance:<InstanceID>], <portNum>]]</p> <p>Описание параметров: InstanceID: ID экземпляра. portNum: ID порта.</p>	Уведомление
<p>Описание события: статус порта Spanning Tree изменился.</p> <p>Сообщение в журнале: Spanning Tree port status change [[[Instance:<InstanceID>], <portNum>]] <old_status> -> <new_status> Описание параметров: InstanceID: ID экземпляра. portNum: ID порта. old_status: предыдущий статус. new_status: новый статус.</p>	Уведомление
<p>Описание события: роль порта Spanning Tree изменилась.</p> <p>Сообщение в журнале: Spanning Tree port role change. [[[Instance:<InstanceID>], <portNum>]] <old_role> -> <new_role> Описание параметров: InstanceID: ID экземпляра. portNum: ID порта. old_role: предыдущая роль. new_role: новая роль.</p>	Информационный
<p>Описание события: создан экземпляр Spanning Tree.</p> <p>Сообщение в журнале: Spanning Tree instance created. (Instance:<InstanceID>) Описание параметров:</p>	Информационный

InstanceID: ID экземпляра.	
Описание события: удален экземпляр Spanning Tree. Сообщение в журнале: Spanning Tree instance deleted. (Instance:<InstanceID>) Описание параметров: InstanceID: ID экземпляра.	Информационный
Описание события: версия Spanning Tree изменилась. Сообщение в журнале: Spanning Tree version change.(New version:<new_version>) Описание параметров: new_version: новая версия STP.	Информационный
Описание события: ID конфигурации MST Spanning Tree и revision level изменились. Сообщение в журнале: Spanning Tree MST configuration ID name and revision level change (name:<name> revision level <revision_level>). Описание параметров: revision_level: новый уровень ревизии.	Информационный
Описание события: таблица соответствия Spanning Tree MST configuration ID VLAN удалена. Сообщение в журнале: Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> delete vlan <startvlanid> [- <endvlanid>]). Описание параметров: InstanceID: ID экземпляра. startvlanid- endvlanid: список VLAN.	Информационный
Описание события: таблица соответствия Spanning Tree MST configuration ID VLAN добавлена. Сообщение в журнале: Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> add vlan <startvlanid> [- <endvlanid>]). Описание параметров: InstanceID: ID экземпляра. startvlanid- endvlanid: список VLAN.	Информационный
Описание события: порту Spanning Tree была присвоена роль альтернативного порта (Alternate Port) из-за STP Root Guard. Сообщение в журнале: Spanning Tree port role change (Instance : <InstanceID>, <portNum>) to alternate port due to the guard root. Описание параметров: InstanceID: ID экземпляра. portNum: ID порта.	Информационный
Описание события: состояние «Blocking» Spanning Tree Loop Guard. Сообщение в журнале: Spanning Tree loop guard blocking(Instance : <InstanceID>, <portNum>) Описание параметров: InstanceID: ID экземпляра. portNum: ID порта.	Информационный

Peripheral

Описание записей журнала	Уровень
<p>Описание события: вентилятор восстановлен.</p> <p>Сообщение в журнале: Unit <unit-id>, <fan-descr> back to normal</p> <p>Описание параметров:</p> <p>Unit <id>: Unit ID.</p> <p><fan-descr>: например, Right Fan, Left Fan и т.д.</p>	Критический
<p>Описание события: вентилятор вышел из строя. Сообщение в журнале: Unit <unit-id> <fan-descr> failed.</p> <p>Описание параметров:</p> <p>Unit <id>: ID устройства.</p> <p><fan-descr>: например, Right Fan, Left Fan и т.д.</p>	Критический
<p>Описание события: датчик температуры показывает критическое значение. Сообщение в журнале: Unit <unit-id> <thermal-sensor-descr> detects abnormal temperature <degree></p> <p>Описание параметров:</p> <p>Unit <id>: ID устройства.</p> <p>thermal-sensor-descr: описание датчика.</p> <p>degree: текущая температура, отображаемая датчиком.</p>	Предупреждение
<p>Описание события: температура вернулась к нормальному значению. Сообщение в журнале: Unit <unit-id> <thermal-sensor-descr> temperature back to normal</p> <p>Описание параметров:</p> <p>Unit <id>: ID устройства.</p> <p>thermal-sensor-descr: описание датчика.</p> <p>degree: текущая температура, отображаемая датчиком.</p>	Информационный
<p>Описание события: отказ питания.</p> <p>Сообщение в журнале: Unit <unit-id> <power-descr> failed</p> <p>Описание параметров:</p> <p>Unit <id>: ID устройства.</p> <p>power-descr: описание питания.</p>	Критический
<p>Описание события: восстановление питания.</p> <p>Сообщение в журнале: Unit <unit-id> <power-descr> back to normal</p> <p>Описание параметров:</p> <p>Unit <id>: ID устройства.</p> <p>power-descr: описание питания.</p>	Критический
<p>Описание события: состояние External Alarm изменилось.</p> <p>Сообщение в журнале: Unit <unit-id> External Alarm Channel <channelID> :<alarmMsg></p> <p>Описание параметров: Unit <id>: ID устройства. ChannelID: ID канала. alarmMsg: Alarm Msg.</p>	Критический

Port

Описание записей журнала	Уровень
<p>Описание события: соединение на порту установлено.</p> <p>Сообщение в журнале: Port <port> link up, <nway></p> <p>Описание параметров:</p>	Информационный

параметров:

port: номер логического порта.

nway: скорость и режим дуплекса соединения.

Описание события: соединение на порту прервано.

Информационный

Сообщение в журнале: Port <port> link down

Описание параметров:

port: номер логического порта.

Port Security

Описание записей журнала

Уровень

Описание события: превышено максимальное количество адресов на порту. Сообщение в журнале: MAC address <mac-address> causes port security violation on <interface-id>.

Предупреждение

Описание параметров:

macaddr: недопустимый MAC-адрес. interface-id: имя интерфейса.

Описание события: превышено максимальное количество адресов в системе. Сообщение в журнале: Limit on system entry number has been exceeded.

Предупреждение

Reboot Schedule

Описание записей журнала

Уровень

Описание события: рекомендованное значение времени для перезагрузки коммутатора.

Критический

Сообщение в журнале: Display "Reboot scheduled in 5 minutes" when the countdown equals 5 minutes. Display "Reboot scheduled in 1 minute" when the countdown equals 1 minute..

Safeguard

Описание записей журнала

Уровень

Описание события: загрузка CPU превысила верхний порог, коммутатор перешел в режим высокой загрузки.

Предупреждение

Сообщение в журнале: Unit <unit-id>, Safeguard Engine enters EXHAUSTED mode. Описание параметров:

unit-id: Unit ID.

Описание события: загрузка CPU снизилась до нижнего порога, коммутатор перешел в нормальный режим.

Информационный

Сообщение в журнале: Unit <unit-id>, Safeguard Engine enters NORMAL mode. Описание параметров:

unit-id: Unit ID.

SNMP

Описание записей журнала

Уровень

Описание события: получен запрос SNMP с неверной строкой

Информационный

сообщества. Сообщение в журнале: SNMP request received from <ipaddr> with invalid community string.

Описание параметров: ipaddr: IP-адрес.

SSH

Описание записей журнала	Уровень
Описание события: сервер SSH включен. Сообщение в журнале: SSH server is enabled	Информационный
Описание события: сервер SSH отключен. Сообщение в журнале: SSH server is disabled	Информационный

SSL

Описание записей журнала	Уровень
Описание события: успешный вход через Web (SSL). Сообщение в журнале: Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя пользователя, используемое для входа на SSL-сервер. ipaddr: IP-адрес SSL-клиента.	Информационный
Описание события: не удалось выполнить вход через Web (SSL). Сообщение в журнале: Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя пользователя, используемое для входа на SSL-сервер. ipaddr: IP-адрес SSL-клиента.	Предупреждение
Описание события: время сессии Web (SSL) истекло. Сообщение в журнале: Web (SSL) session timed out (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя пользователя, используемое для входа на SSL-сервер. ipaddr: IP-адрес SSL-клиента.	Информационный
Описание события: выполнен выход через Web (SSL). Сообщение в журнале: Logout through Web (SSL) (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя пользователя, используемое для входа на SSL-сервер. ipaddr: IP-адрес SSL-клиента.	Информационный

Stacking

Описание записей журнала	Уровень
Описание события: «горячее» добавление.	Информационный

Сообщение в журнале: Unit: <unitID>, MAC: <macaddr> Hot insertion. Описание параметров: unitID: ID модуля. Macaddr: MAC-адрес.	
Описание события: «горячее» удаление. Сообщение в журнале: Unit: <unitID>, MAC: <macaddr> Hot removal. Описание параметров: unitID: ID модуля. Macaddr: MAC-адрес.	Информационный
Описание события: топология стекирования изменилась. Сообщение в журнале: Stacking topology is <Stack_TP_TYPE>. Master (Unit <unitID>, MAC:<macaddr>). Описание параметров: Stack_TP_TYPE: типы топологии стекирования: Ring (кольцевая), Chain (линейная). unitID: ID модуля. Macaddr: MAC-адрес.	Критический
Описание события: резервное устройство стало основным. Сообщение в журнале: Backup master changed to master. Master (Unit: <unitID>). Описание параметров: unitID: ID модуля.	Информационный
Описание события: дополнительное устройство стало основным. Сообщение в журнале: Slave changed to master. Master (Unit: <unitID>). Описание параметров: unitID: ID модуля.	Информационный
Описание события: неверный Unit ID. Сообщение в журнале: Slave changed to master. Master (Unit: <unitID>). Описание параметров: unitID: ID модуля. macaddr: MAC-адреса неверных Unit ID.	Критический
Описание события: соединение на порту стекирования установлено. Сообщение в журнале: Stacking port <portID> link up. Описание параметров: portID: ID порта.	Критический
Описание события: соединение на порту стекирования прервано. Сообщение в журнале: Stacking port <portID> link down. Описание параметров: portID: ID порта.	Критический
Описание события: соединение с интерфейсом SIO установлено. Сообщение в журнале: SIO interface Unit <unitID> SIO<SIOID> link up. Описание параметров: unitID: ID модуля. SIOID: ID SIO.	Критический
Описание события: соединение с интерфейсом SIO прервано. Сообщение в журнале: SIO interface Unit <unitID> SIO<SIOID> link down. Описание параметров: unitID: ID модуля. SIOID: ID SIO.	Критический

Storm Control

Описание записей журнала	Уровень
<p>Описание события: возникновение шторма.</p> <p>Сообщение в журнале: <Broadcast Multicast Unicast> storm is occurring on <interface-id>. Описание параметров:</p> <p>Broadcast: шторм, возникший из-за широковещательных пакетов (DA = FF:FF:FF:FF:FF:FF).</p> <p>Multicast: шторм, возникший из-за многоадресных пакетов, включая известные и неизвестные пакеты 2 уровня, пакеты с известным и неизвестным IP.</p> <p>Unicast: шторм, возникший из-за одноадресных пакетов, включая известные и неизвестные пакеты.</p> <p>interface-id: ID интерфейса, на котором возник шторм.</p>	Предупреждение
<p>Описание события: шторм устранен.</p> <p>Сообщение в журнале: <Broadcast Multicast Unicast> storm is cleared on <interface-id>. Описание параметров:</p> <p>Broadcast: устранен шторм широковещательных пакетов (Broadcast Storm). Multicast: устранен шторм многоадресных пакетов (Multicast Storm).</p> <p>Unicast: устранен шторм одноадресных пакетов, включая известные и неизвестные пакеты (Unicast Storm).</p> <p>interface-id: ID интерфейса, на котором шторм устранен</p>	Информационный
<p>Описание события: соединение на порту прервано из-за возникновение шторма. Сообщение в журнале: <interface-id> is currently shut down due to the <Broadcast Multicast Unicast> storm.</p> <p>Описание параметров:</p> <p>interface-id: ID интерфейса, находящегося в состоянии Error-Disabled из-за шторма.</p> <p>Broadcast: интерфейс отключен из-за шторма широковещательных пакетов. Multicast: интерфейс отключен из-за шторма многоадресных пакетов.</p> <p>Unicast: интерфейс отключен из-за шторма одноадресных пакетов, включая известные и неизвестные пакеты.</p>	Предупреждение

Telnet

Описание записей журнала	Уровень
<p>Описание события: успешный вход через Telnet.</p> <p>Сообщение в журнале: Successful login through Telnet (Username: <username>, IP: <ipaddr>)</p> <p>Описание параметров:</p> <p>ipaddr: IP-адрес Telnet-клиента.</p> <p>username: имя пользователя, используемое для входа на</p>	Информационный

Telnet-сервер.	
<p>Описание события: не удалось выполнить вход через Telnet. Сообщение в журнале: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Описание параметров: ipaddr: IP-адрес Telnet-клиента. username: имя пользователя, используемое для входа на Telnet-сервер.</p>	Предупреждение
<p>Описание события: выполнен выход через Telnet. Сообщение в журнале: Logout through Telnet (Username: <username>, IP: <ipaddr>) Описание параметров: ipaddr: IP-адрес Telnet-клиента. username: имя пользователя, используемое для входа на Telnet-сервер.</p>	Информационный
<p>Описание события: время сессии Telnet истекло. Сообщение в журнале: Telnet session timed out (Username: <username>, IP: <ipaddr>). Описание параметров: ipaddr: IP-адрес Telnet-клиента. username: имя пользователя, используемое для входа на Telnet-сервер.</p>	Информационный

Traffic Control

Описание записей журнала	Уровень
<p>Описание события: возникновение шторма широковещательных пакетов. Сообщение в журнале: <interface-id> Broadcast storm is occurring. Описание параметров: interface-id: имя интерфейса.</p>	Предупреждение
<p>Описание события: шторм широковещательных пакетов устранен. Сообщение в журнале: <interface-id> Broadcast storm has cleared. Описание параметров: interface-id: имя интерфейса.</p>	Информационный
<p>Описание события: возникновение шторма многоадресных пакетов. Сообщение в журнале: <interface-id> Multicast storm is occurring. Описание параметров: interface-id: имя интерфейса.</p>	Предупреждение
<p>Описание события: шторм многоадресных пакетов устранен. Сообщение в журнале: <interface-id> Multicast storm has cleared. Описание параметров: interface-id: имя интерфейса.</p>	Информационный
<p>Описание события: возникновение шторма одноадресных пакетов. Сообщение в журнале: <interface-id> Unicast storm is</p>	Предупреждение

occurring.	
Описание параметров: interface-id: имя интерфейса.	
Описание события: шторм одноадресных пакетов устранен. Сообщение в журнале: <interface-id> Unicast storm has cleared. Описание параметров: interface-id: имя интерфейса.	Информационный
Описание события: соединение на порту прервано из-за возникновения шторма. Сообщение в журнале: <interface-id> is currently shut down due to a packet storm. Описание параметров: interface-id: имя интерфейса.	Предупреждение

VRRP Debug Enhancement

Описание записей журнала	Уровень
Описание события: один виртуальный маршрутизатор перешел в режим Master. Сообщение в журнале: VR <vr-id> at interface <intf-name> Switch to Master Описание параметров: vr-id: ID виртуального маршрутизатора VRRP. intf-name: имя интерфейса, на котором настроен виртуальный маршрутизатор.	Информационный
Описание события: один виртуальный маршрутизатор перешел в режим Backup. Сообщение в журнале: VR <vr-id> at interface <intf-name> Switch to Backup Описание параметров: vr-id: ID виртуального маршрутизатора VRRP. intf-name: имя интерфейса, на котором настроен виртуальный маршрутизатор.	Информационный
Описание события: один виртуальный маршрутизатор перешел в режим Init. Сообщение в журнале: VR <vr-id> at interfaОписание параметров: vr-id: ID виртуального маршрутизатора VRRP. intf-name: имя интерфейса, на котором настроен виртуальный маршрутизатор.ce <intf-name> Switch to Init	Информационный
Описание события: получено одно сообщение VRRP-Advertisement, которое не соответствует заданному типу аутентификации. Сообщение в журнале: Authentication type mismatch on VR <vr-id> at interface <intf-name> Описание параметров: vr-id: ID виртуального маршрутизатора VRRP. intf-name: имя интерфейса, на котором настроен виртуальный маршрутизатор.	Предупреждение
Описание события: одно полученное сообщения VRRP-Advertisement не прошло аутентификацию. Сообщение в журнале: Authentication fail on VR <vr-id> at interface <intf-name>. Auth type <auth-type>	Предупреждение

<p>Описание параметров:</p> <p>vr-id: ID виртуального маршрутизатора VRRP.</p> <p>intf-name: имя интерфейса, на котором настроен виртуальный маршрутизатор. Auth-type: тип аутентификации интерфейса VRRP.</p>	
<p>Описание события: получено одно сообщение VRRP-Advertisement с неверной Checksum.</p> <p>Сообщение в журнале: Received an ADV msg with incorrect checksum on VR <vr-id> at interface <intf-name></p> <p>Описание параметров:</p> <p>vr-id: ID виртуального маршрутизатора VRRP.</p> <p>intf-name: имя интерфейса, на котором настроен виртуальный маршрутизатор.</p>	Предупреждение
<p>Описание события: получено одно сообщение VRRP-Advertisement с неверным ID виртуального маршрутизатора.</p> <p>Сообщение в журнале: Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name></p> <p>Описание параметров:</p> <p>vr-id: ID виртуального маршрутизатора VRRP.</p> <p>intf-name: имя интерфейса, на котором настроен виртуальный маршрутизатор.</p>	Предупреждение
<p>Описание события: получено одно сообщения VRRP-Advertisement, которое не соответствует заданному интервалу.</p> <p>Сообщение в журнале: Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name></p> <p>Описание параметров:</p> <p>vr-id: ID виртуального маршрутизатора VRRP.</p> <p>intf-name: имя интерфейса, на котором настроен виртуальный маршрутизатор.</p>	Предупреждение
<p>Описание события: в таблице 2 уровня добавлен виртуальный MAC-адрес. Сообщение в журнале: Added a virtual MAC <vrrp-mac-addr> into L2 table</p> <p>Описание параметров:</p> <p>vrrp-mac-addr: виртуальный MAC-адрес VRRP.</p>	Уведомление
<p>Описание события: из таблицы 2 уровня удален виртуальный MAC-адрес. Сообщение в журнале: Deleted a virtual MAC <vrrp-mac-addr> from L2 table</p> <p>Описание параметров:</p> <p>vrrp-mac-addr: виртуальный MAC-адрес VRRP.</p>	Уведомление
<p>Описание события: в таблицу 3 уровня добавлен виртуальный MAC-адрес. Сообщение в журнале: Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table</p> <p>Описание параметров:</p> <p>vrrp-ip-addr: виртуальный IP-адрес VRRP.</p> <p>vrrp-mac-addr: виртуальный MAC-адрес VRRP.</p>	Уведомление
<p>Описание события: из таблицы 3 уровня удален виртуальный MAC-адрес. Сообщение в журнале: Deleted a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from L3 table</p> <p>Описание параметров:</p>	Уведомление

<p>vrrp-ip-addr: виртуальный IP-адрес VRRP. vrrp-mac-addr: виртуальный MAC-адрес VRRP.</p>	
<p>Описание события: не удалось добавить виртуальный MAC-адрес в таблицу 2 уровня чипсета коммутатора. Сообщение в журнале: Failed to add virtual MAC <vrrp-mac-addr> into chip L2 table. Errcode <vrrp-errcode> Описание параметров: vrrp-mac-addr: виртуальный MAC-адрес VRRP. vrrp-errcode: errcode протокола VRRP.</p>	Ошибка
<p>Описание события: не удалось удалить виртуальный MAC-адрес из таблицы 2 уровня чипсета коммутатора. Сообщение в журнале: Failed to delete virtual MAC <vrrp-mac-addr> from chip L2 table. Errcode <vrrp-errcode> Описание параметров: vrrp-mac-addr: виртуальный MAC-адрес VRRP. vrrp-errcode: errcode протокола VRRP.</p>	Ошибка
<p>Описание события: не удалось добавить виртуальный MAC-адрес в таблицу 3 уровня. Таблица 3 уровня заполнена. Сообщение в журнале: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. L3 table is full Описание параметров: vrrp-ip-addr: виртуальный IP-адрес VRRP. vrrp-mac-addr: виртуальный MAC-адрес VRRP.</p>	Ошибка
<p>Описание события: не удалось добавить виртуальный MAC-адрес в таблицу 3 уровня. Порт, с которого был получен MAC-адрес, недействителен. Сообщение в журнале: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Port <mac-port> is invalid Описание параметров: vrrp-ip-addr: виртуальный IP-адрес VRRP. vrrp-mac-addr: виртуальный MAC-адрес VRRP. mac-port: номер порта виртуального MAC-адреса VRRP.</p>	Ошибка
<p>Описание события: не удалось добавить виртуальный MAC-адрес в таблицу 3 уровня. Интерфейс, с которого был получен MAC-адрес, недействителен. Сообщение в журнале: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Interface <mac-intf> is invalid Описание параметров: vrrp-ip-addr: виртуальный IP-адрес VRRP. vrrp-mac-addr: виртуальный MAC-адрес VRRP. mac-port: номер порта виртуального MAC-адреса VRRP.</p>	Ошибка
<p>Описание события: не удалось добавить виртуальный MAC-адрес в таблицу 3 уровня. Unit ID устройства, с которого был получен MAC-адрес, недействителен. Сообщение в журнале: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr></p>	Ошибка

<p>into L3 table. Box id <mac-box> is invalid</p> <p>Описание параметров:</p> <p>vrrp-ip-addr: виртуальный IP-адрес VRRP.</p> <p>vrrp-mac-addr: виртуальный MAC-адрес VRRP. Ошибка</p> <p>mac-box: номер устройства в стеке виртуального MAC- Ошибка адреса VRRP.</p>	
<p>Описание события: не удалось добавить виртуальный MAC-адрес в таблицу 3 уровня чипсета. Сообщение в журнале: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into chip L3 table. Errcode <vrrp-errcode></p> <p>Описание параметров:</p> <p>vrrp-ip-addr: виртуальный IP-адрес VRRP.</p> <p>vrrp-mac-addr: виртуальный MAC-адрес VRRP. vrrp-errcode: errcode протокола VRRP.</p>	Ошибка
<p>Описание события: не удалось удалить виртуальный MAC-адрес из таблицы 3 уровня чипсета.</p> <p>Сообщение в журнале: Failed to delete virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from chip L3 table. Errcode <vrrp-errcode></p> <p>Описание параметров:</p> <p>vrrp-mac-addr: виртуальный MAC-адрес VRRP. vrrp-errcode: errcode протокола VRRP.</p>	Ошибка

WAC

Описание записей журнала	Уровень
<p>Описание события: хосту не удалось пройти аутентификацию.</p> <p>Сообщение в журнале: WAC unauthenticated user (User Name: <string>, IP: <ipaddr ipv6address>, MAC: <macaddr>, Port: <[unitID:]portNum>)</p> <p>Описание параметров:</p> <p>string: имя пользователя. ipaddr: IP-адрес. ipv6address: IPv6-адрес. macaddr: MAC-адрес. unitID: Unit ID.</p> <p>portNum: номер порта.</p>	Предупреждение
<p>Описание события: количество авторизованных пользователей на устройстве превысило максимальное значение.</p> <p>Сообщение в журнале: WAC enters stop learning state.</p>	Предупреждение
<p>Описание события: количество авторизованных пользователей на устройстве через определенный интервал времени вернулось к значению ниже максимального.</p> <p>Сообщение в журнале: WAC recovered from stop learning state.</p>	Предупреждение
<p>Описание события: хост успешно прошел аутентификацию.</p> <p>Сообщение в журнале: WAC authenticated user (Username: <string>, IP: <ipaddr ipv6address>, MAC: <macaddr>, Port: <[unitID:] portNum>)</p> <p>Описание параметров: string: имя пользователя. ipaddr: IP-адрес. ipv6address: IPv6-адрес. macaddr: MAC-адрес. unitID: Unit ID.</p>	Предупреждение

portNum: номер порта.

Web

Описание записей журнала	Уровень
<p>Описание события: успешный вход через Web. Сообщение в журнале: Successful login through Web (Username: <username>, IP: <ipaddr>).</p> <p>Описание параметров: username: имя пользователя, используемое для входа на HTTP-сервер. ipaddr: IP-адрес HTTP-клиента.</p>	Информационный
<p>Описание события: не удалось войти через Web.</p> <p>Сообщение в журнале: Login failed through Web (Username: <username>, IP: <ipaddr>).</p> <p>Описание параметров: username: имя пользователя, используемое для входа на HTTP-сервер. ipaddr: IP-адрес HTTP-клиента.</p>	Предупреждение
<p>Описание события: время сессии Web истекло.</p> <p>Сообщение в журнале: Web session timed out (Username: <username>, IP: <ipaddr>).</p> <p>Описание параметров: username: имя пользователя, используемое для входа на HTTP-сервер. ipaddr: IP-адрес HTTP-клиента.</p>	Информационный
<p>Описание события: выполнен выход через Web.</p> <p>Сообщение в журнале: Logout through Web (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя пользователя, используемое для входа на HTTP-сервер. ipaddr: IP-адрес HTTP-клиента.</p>	Информационный

Приложение В. Записи trap-сообщений

Таблица ниже содержит все возможные записи trap-сообщений и их соответствующие значения, встречающиеся на коммутаторе.

802.1X

Сообщение trap	Описание	OID
dDot1xExtLoggedSuccess	Хост прошел аутентификацию 802.1X. Вариабельные привязки: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName	1.3.6.1.4.1.17 1.14.30.0.1
dDot1xExtLoggedFail	Хост не прошел аутентификацию 802.1X. Вариабельные привязки: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName (5) dDot1xExtNotifyFailReason	1.3.6.1.4.1.17 1.14.30.0.2

802.3 ah OAM

Сообщение trap	Описание	OID
dot3OamThresholdEvent	Локальное или удаленное устройство превысило заданный порог. Вариабельные привязки: (1) dot3OamEventLogTimestamp (2) dot3OamEventLogOui (3) dot3OamEventLogType (4) dot3OamEventLogLocation (5) dot3OamEventLogWindowHi (6) dot3OamEventLogWindowLo (7) dot3OamEventLogThresholdHi (8) dot3OamEventLogThresholdLo (9) dot3OamEventLogValue	1.3.6.1. 2.1.158. 0.1

	(10) dot3OamEventLogRunningTotal	
	(11) dot3OamEventLogEventTotal	
dot3OamNonThresholdEvent	Локальное или удаленное устройство не превысило заданный порог. Вариабельные привязки: (1) dot3OamEventLogTimestamp (2) dot3OamEventLogOui (3) dot3OamEventLogType (4) dot3OamEventLogLocation (5) dot3OamEventLogEventTotal	1.3.6.1. 2.1.158. 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

BPDU Protection

Сообщение trap	Описание	OID
dBpduProtectionAttackOccur	Атака BPDU на интерфейсе. Вариабельные привязки: (1) ifIndex (2) dBpduProtectionIfCfgMode	1.3.6.1.4.1.17 1.14.47.0.1
dBpduProtectionAttackRecover	Атака BPDU на интерфейсе устранена. Вариабельные привязки: (1) ifIndex	1.3.6.1.4.1.17 1.14.47.0.2

CFM

Сообщение trap	Описание	OID
dot1agCfmFaultAlarm	Обнаружена ошибка подключения. Вариабельные привязки: (1) ifIndex	1.3.111.2.802. 1.1.8.0.1

Расширение CFM

Сообщение trap	Описание	OID
dCfmAisOccurred	Локальная MEP перешла в статус AIS. Вариабельные привязки: (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMeplIdentifier	1.3.6.1.4.1.17 1.14.86.0.1
dCfmAisCleared	Локальная MEP вышла из статуса AIS. Вариабельные привязки: (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMeplIdentifier	1.3.6.1.4.1.17 1.14.86.0.2
dCfmLockOccurred	Локальная MEP перешла в состояние «Lock». Вариабельные привязки: (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMeplIdentifier	1.3.6.1.4.1.17 1.14.86.0.3
dCfmLockCleared	Локальная MEP вышла из состояния «Lock». Вариабельные привязки: (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMeplIdentifier	1.3.6.1.4.1.17 1.14.86.0.4

DDM

Сообщение trap	Описание	OID
dDdmAlarmTrap	Возникновение проблем уровня alarm или возвращение к нормальному состоянию после устранения данных проблем. Trap-сообщение об устранении проблем будет отправлено, если текущее значение выше заданного нижнего порога alarm или ниже заданного верхнего порога alarm. Вариабельные привязки: (1) dDdmNotifyInfoIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.17 1.14.72.0.1
dDdmWarningTrap	Возникновение проблем уровня warning или возвращение к нормальному состоянию после устранения данных проблем. Вариабельные привязки:	1.3.6.1.4.1.17 1.14.72.0.2

(1) dDdmNotifyInfoIndex,
 (2) dDdmNotifyInfoComponent
 (3) dDdmNotifyInfoAbnormalLevel
 (4)
 dDdmNotifyInfoThresholdExceedOrRecover

DHCP Server Screen Prevention

Сообщение trap	Описание	OID
dDhcpFilterAttackDetected	Если функция DHCP Server Screen включена, trap-сообщения будут отправлены при получении каждого пакета ложного DHCP-сервера. Вариабельные привязки: (1) dDhcpFilterLogBufServerIpAddr (2) dDhcpFilterLogBufClientMacAddr (3) dDhcpFilterLogBufferVlanId (4) dDhcpFilterLogBufferOccurTime	1.3.6.1.4.1.17 1.14.133.0.1

DoS Prevention

Сообщение trap	Описание	OID
dDosPreveAttackDetectedPacket	Обнаружена DoS-атака. Вариабельные привязки: (1) dDoSPrevCtrlAttackType (2) dDosPrevNotiInfoDropIpAddr (3) dDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.17 1.14.59.0.2

ERPS

Сообщение trap	Описание	OID
dErpsFailedetectedNotif	Обнаружено отсутствие сигнала. Трап-сообщение об отсутствии сигнала будет отправлено, если ранее параметр dErpsNotificationEnabled был включен.	1.3.6.1.4.1.1 7 1.14.78.0.1
dErpsFailureClearedNotif	Отсутствие сигнала устранено. Трап-сообщение об устранении отсутствия сигнала будет отправлено, если ранее параметр dErpsNotificationEnabled был включен.	1.3.6.1.4.1.1 7 1.14.78.0.2

dErpsRPLOwnerConflictNotif	Конфликт RPL owner. Trap-сообщение о конфликте RPL owner будет отправлено, если ранее параметр dErpsNotificationEnabled был включен.	1.3.6.1.4.1.1 7 1.14.78.0.3
----------------------------	--	-----------------------------------

ErrDisable

Сообщение trap	Описание	OID
dErrDisNotifyPortDisabledAssert	Порт перешел в состояние Error-Disabled. Вариабельные привязки: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.17 1.14.45.0.1
dErrDisNotifyPortDisabledClear	Порт возвращается в исходное состояние по истечению определенного интервала времени. Вариабельные привязки: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.17 1.14.45.0.2

Gratuitous ARP

Сообщение trap	Описание	OID
agentGratuitousARPTrap	Обнаружен конфликт IP-адреса. Вариабельные привязки: (1) ipaddr (2) macaddr (3) portNumber (4) agentGratuitousARPInterfaceName	1.3.6.1.4.1.17 1.14.45.0.1

IP-MAC-Port Binding

Сообщение trap	Описание	OID
dImpbViolationTrap	Обнаружен недопустимый адрес привязки IP-MAC-Port Binding. Вариабельные привязки: (1) ifIndex (2) dImpbViolationIpAddrType (3) dImpbViolationIpAddress (4) dImpbViolationMacAddress (5) dImpbViolationVlan	1.3.6.1.4.1.17 1.14.22.0.1

LACP

Сообщение trap	Описание	OID
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
swPortLoopOccurred	Обнаружена петля. Вариабельные привязки: (1) swLoopDetectPortIndex	1.3.6.1.4.1.17 1.14.46.0.1
swPortLoopRestart	Порт возвращается в исходное состояние по истечению определенного интервала времени. Вариабельные привязки: (1) swLoopDetectPortIndex	1.3.6.1.4.1.17 1.14.46.0.2
swVlanLoopOccurred	Обнаружена петля в режиме LBD VLAN-Based. Вариабельные привязки: (1) swLoopDetectPortIndex (2) swVlanLoopDetectVID	1.3.6.1.4.1.17 1.14.46.0.3
swVlanLoopRestart	Порт возвращается в исходное состояние в режиме LBD VLAN-based по истечению определенного интервала времени. Вариабельные привязки: (1) swLoopDetectPortIndex (2) swVlanLoopDetectVID	1.3.6.1.4.1.17 1.14.46.0.4

LLDP-MED

Сообщение trap	Описание	OID
IldpRemTablesChange	Значение IldpStatsRemTableLastChangeTime изменилось. Варибельные привязки: (1) IldpStatsRemTablesInserts (2) IldpStatsRemTablesDeletes (3) IldpStatsRemTablesDrops (4) IldpStatsRemTablesAgeouts	1.0.8802.1.1.2 .0.0.1
IldpXMedTopologyChangeDetected	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) IldpRemChassisIdSubtype (2) IldpRemChassisId (3) IldpXMedRemDeviceClass	1.0.8808.1.1.2 .1.5.4795.0.1

MAC-based Access Control

Сообщение trap	Описание	OID
dMacAuthLoggedSuccess	Хост успешно прошел аутентификацию на основе MAC. Варибельные привязки: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.17 1.14.153.0.1
dMacAuthLoggedFai	Хост не прошел аутентификацию на основе MAC. Варибельные привязки: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.17 1.14.153.0.2
dMacAuthLoggedAgesOut	Время аутентификации хоста истекло. (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.17 1.14.153.0.3

MAC Notification

Сообщение trap	Описание	OID
dL2FdbMacNotification	Изменение MAC-адресов в таблице коммутации. Варибельные привязки: (1) dL2FdbMac ChangeNotifyInfo	1.3.6.1.4.1.17 1.14.3.0.1

dL2FdbMacNotificationWithVID	Изменение MAC-адресов в таблице коммутации с VLAN ID. Вариабельные привязки: (1) dL2FdbMacChangeNotifyInfoWithVID	1.3.6.1.4.1.17 1.14.3.0.2
------------------------------	---	------------------------------

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	Вентилятор вышел из строя. Данное trap-сообщение отправляется Commander Switch. Уведомление dEntityExtEnvFanStatus может быть «fault», а при восстановлении вентилятора – «ok». Вариабельные привязки: (1) dEntityExtEnvFanUnitId (2) dEntityExtEnvFanIndex (3) dEntityExtEnvFanStatus	1.3.6.1.4.1.17 1.14.5.0.1
dEntityExtThermalStatusChg	Датчик температуры показывает критическое значение. Данное trap-сообщение отправляется Commander Switch. Уведомление dEntityExtEnvTempStatus может быть «abnormal», а при возвращении температуры к нормальному значению – «ok».	1.3.6.1.4.1.17 1.14.5.0.2

	<p>Вариабельные привязки: (1) dEntityExtEnvTempUnitId (2) dEntityExtEnvTempIndex (3) dEntityExtEnvTempStatus</p>	
dEntityExtPowerStatusChg	<p>Выход из строя, удаление или восстановление модуля питания. Данное trap-сообщение отправляется Commander Switch.</p> <p>Вариабельные привязки: (1) dEntityExtEnvPowerUnitId (2) dEntityExtEnvPowerIndex (3) dEntityExtEnvPowerStatus</p>	<p>1.3.6.1.4.1.17 1.14.5.0.3</p>

Port Security

Сообщение trap	Описание	OID
dPortSecMacAddrViolation	<p>Если отправка trap-сообщений Port Security включена, trap-сообщения будут отправлены при обнаружении недопустимых MAC-адресов.</p> <p>Вариабельные привязки: (1) ifIndex, (2) dPortSecIfCurrentStatus (3) dPortSecIfViolationMacAddress</p>	<p>1.3.6.1.4.1.17 1.14.8.0.1</p>

Port

Сообщение trap	Описание	OID
linkUp	<p>Соединение на порту установлено.</p> <p>Вариабельные привязки: (1) ifIndex, (2) if AdminStatus (3) ifOperStatus</p>	<p>1.3.6.1.6.3.1.1 .5.4</p>
linkDown	<p>Соединение на порту прервано.</p> <p>Вариабельные привязки: (1) ifIndex, (2) if AdminStatus (3) ifOperStatus</p>	<p>1.3.6.1.6.3.1.1 .5.3</p>

Reboot Schedule

Сообщение trap	Описание	OID
agentRebootIn5Min	Значение таймера Countdown достигло 5 минут.	<p>1.3.6.1.4.1.17 1.14.170.0.1</p>
agentRebootIn1Min	Значение таймера Countdown достигло 1	1.3.6.1.4.1.17

минуты.

1.14.170.0.2

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 изменился на режим высокой загрузки. Вариабельные привязки: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.17 1.14.19.1.1.0. 1
dSafeguardChgToNormal	Режим высокой загрузки системы изменился на нормальный режим. Вариабельные привязки: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.17 1.14.19.1.1.0. 2

SIM

Сообщение trap	Описание	OID
swSingleIPMSColdStart	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление о «холодном» старте. Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.11
swSingleIPMSWarmStart	Данное trap-сообщений будет	1.3.6.1.4.1.17

	отправлено Commander Switch, если участником его группы было сгенерировано уведомление о «горячем» старте. Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.12.8.6.0.12
swSingleIPMSLinkDown	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление о прерванном соединении. Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.17 1.12.8.6.0.13
swSingleIPMSLinkUp	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление об установленном соединении. Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.17 1.12.8.6.0.14
swSingleIPMSAuthFail	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление об ошибки аутентификации. Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.15
swSingleIPMSnewRoot	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление о новом корне. Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.16
swSingleIPMSTopologyChange	Данное trap-сообщений будет отправлено Commander Switch, если участником его	1.3.6.1.4.1.17 1.12.8.6.0.17

группы было сгенерировано уведомление об изменении топологии.

Вариабельные привязки:

(1) swSingleIPMSID

(2) swSingleIPMSMacAddr

Stacking

Сообщение trap	Описание	OID
dStackInsertNotification	«Горячее» добавление модуля. Вариабельные привязки: (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.17 1.14.9.0.1
dStackRemoveNotification	«Горячее» удаление модуля. Вариабельные привязки: (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.17 1.14.9.0.2
dStackFailureNotification	Ошибка подключения модуля. Вариабельные привязки: (1) dStackNotifyInfoBoxId	1.3.6.1.4.1.17 1.14.9.0.3
dStackTPChangeNotification	Изменение топологии стекирования. Вариабельные привязки: (1) dStackNotifyInfoTopologyType (2) dStackNotifyInfoBoxId (3) dStackInfoMacAddr	1.3.6.1.4.1.17 1.14.9.0.4
dStackRoleChangeNotification	Изменение роли модуля в стеке. Вариабельные привязки: (1) dStackNotifyInfoRoleChangeType (2) dStackNotifyInfoBoxId	1.3.6.1.4.1.17 1.14.9.0.5

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

Storm Control

Сообщение trap	Описание	OID
dStormCtrlOccurred	Данное trap-сообщение будет отправлено, если параметр dStormCtrlNotifyEnable имеет значение «stormOccurred» или «both», а также при возникновении шторма. Вариабельные привязки: (1) ifIndex, (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.17 1.14.25.0.1
dStormCtrlStormCleared	Данное trap-сообщение будет отправлено, если параметр dStormCtrlNotifyEnable имеет значение «stormCleared» или «both», а также при устранении шторма. Вариабельные привязки: (1) ifIndex, (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.17 1.14.25.0.2

System File

Сообщение trap	Описание	OID
dsfUploadImage	Пользователь успешно выгрузил файл образа.	1.3.6.1.4.1.17 1.14.14.0.1
dsfDownloadImage	Пользователь успешно загрузил файл образа.	1.3.6.1.4.1.17 1.14.14.0.2
dsfUploadCfg	Пользователь успешно выгрузил конфигурационный файл.	1.3.6.1.4.1.17 1.14.14.0.3
dsfDownloadCfg	Пользователь успешно загрузил конфигурационный файл.	1.3.6.1.4.1.17 1.14.14.0.4
dsfSaveCfg	Пользователь успешно сохранил конфигурационный файл.	1.3.6.1.4.1.17 1.14.14.0.5

Upload/Download

Сообщение trap	Описание	OID
agentFirmwareUpgrade	Завершение процесса обновления ПО через SNMP. Вариабельные привязки: (1) swMultiImageVersion	1.3.6.1.4.1.17 1.12.1.7.2.0.7
agentCfgOperCompleteTrap	Настройки полностью сохранены, выгружены или загружены. Вариабельные привязки: (1) unitID (2) agentCfgOperate (3) agentLoginUserName	1.3.6.1.4.1.17 1.12.1.7.2.0.9

VRRP

Сообщение trap	Описание	OID
vrrpTrapNewMaster	Переход устройства в режим Master. Вариабельные привязки: (1) vrrpOperMasterIpAddr	1.3.6.1.2.1.68. 0.1
vrrpTrapAuthFailure	Маршрутизатором был получен пакет, ключ аутентификации или тип аутентификации которого конфликтует с ключом аутентификации или типом аутентификации этого маршрутизатора. Отправка данного trap-сообщения является опциональной. Вариабельные привязки: (1) vrrpTrapPacketSrc (2) vrrpTrapAuthErrorType	1.3.6.1.2.1.68. 0.2

WAC

Сообщение trap	Описание	OID
swWACLoggedSuccess	WAC-клиент успешно прошел аутентификацию. Вариабельные привязки: (1) swWACAuthStatePort (2) swWACAuthStateOriginalVid (3) swWACAuthStateMACAddr (4) swWACAuthUserName (5) swWACClientAddrType (6) swWACClientAddress	1.3.6.1.4.1.17 1.14.154.0.1
swWACLoggedFail	WAC-клиенту не удалось пройти аутентификацию. Вариабельные привязки: (1) swWACAuthStatePort (2) swWACAuthStateOriginalVid (3) swWACAuthStateMACAddr (4) swWACAuthUserName (5) swWACClientAddrType (6) swWACClientAddress	1.3.6.1.4.1.17 1.14.154.0.2

Приложение Г. Назначение атрибутов RADIUS

На коммутаторах ТГК-313-24 назначение атрибутов RADIUS используется в следующих модулях: Console, Telnet, SSH, Web, 802.1X, WAC и управление доступом на основе MAC.

Ниже представлены следующие атрибуты RADIUS:

Уровень привилегии

Входящая/исходящая полоса пропускания (Ingress/Egress Bandwidth) Приоритет по умолчанию 802.1p VLAN ACL

Для того, чтобы RADIUS-сервер назначил **уровень привилегии**, необходимо сконфигурировать соответствующие параметры на сервере. В таблице ниже приведены параметры для полосы пропускания.

Атрибуты для производителя (Vendor-Specific attributes):

Атрибут для производителя	Описание	Значение	Использование
Vendor-ID	Определяет производителя	171 (DLINK)	Обязательно
Vendor-Type	Определяет атрибут	1	Обязательно
Attribute-Specific Field	Используется для назначения уровня привилегии пользователя для работы с коммутатором	Диапазон (1-15)	Обязательно

Если пользователь сконфигурировал атрибут уровня привилегии на RADIUS-сервере (например, уровень 15) и аутентификация Console, Telnet, SSH и Web прошла успешно, устройство назначит уровень привилегии пользователю в соответствии со значением на RADIUS-сервере. Однако если пользователь не сконфигурировал атрибут уровня привилегии и аутентификация проходит успешно, устройство не назначит пользователю уровень привилегии. Если атрибут уровня привилегии установлен на значение ниже минимального поддерживаемого значения или выше максимального поддерживаемого значения, уровень привилегии игнорируется.

Для того, чтобы RADIUS-сервер назначил **входящую/исходящую полосу пропускания**, необходимо сконфигурировать соответствующие параметры на сервере. В таблице ниже приведены параметры для полосы пропускания.

Атрибуты для производителя (Vendor-Specific attributes):

Атрибут для производителя	Описание	Значение	Использование
Vendor-ID	Определяет производителя	171 (DLINK)	Обязательно
Vendor-Type	Определяет атрибут	2 (для входящей полосы) 3 (для исходящей полосы)	Обязательно
Attribute-Specific Field	Используется для назначения полосы пропускания порта	Unit (Kbits)	Обязательно

Если пользователь сконфигурировал атрибут полосы пропускания на RADIUS-сервере (например, входящая полоса пропускания 1000 кбит/с) и аутентификация 802.1X прошла успешно, устройство назначит полосу пропускания пользователю в соответствии со значением на RADIUS-сервере. Однако если пользователь не сконфигурировал атрибут полосы пропускания и аутентификация проходит успешно, устройство не назначит пользователю полосу пропускания. Если атрибут полосы пропускания установлен на «0», для эффективной полосы пропускания будет установлен параметр `no_limited`. Если атрибут полосы пропускания установлен на значение ниже нуля или выше максимального поддерживаемого значения, полоса пропускания игнорируется.

Для того, чтобы RADIUS-сервер назначил **приоритет по умолчанию 802.1p**, необходимо сконфигурировать соответствующие параметры на сервере. В таблице ниже приведены параметры для приоритета 802.1p.

Атрибуты для производителя (Vendor-Specific attributes):

Атрибут для производителя	Описание	Значение	Использование
Vendor-ID	Определяет производителя	171 (DLINK)	Обязательно
Vendor-Type	Определяет атрибут	4	Обязательно
Attribute-Specific Field	Используется для назначения приоритета по умолчанию 802.1p порта	0-7	Обязательно

Если пользователь сконфигурировал атрибут приоритета 802.1p на RADIUS-сервере (например, приоритет 7) и аутентификация 802.1X или на основе MAC прошла успешно, устройство назначит порту приоритет по умолчанию в соответствии со значением на RADIUS-сервере. Однако если пользователь не сконфигурировал атрибут приоритета и аутентификация проходит успешно, устройство не назначит порту приоритет. Если атрибут приоритета на RADIUS-сервере установлен на значение вне диапазона (>7), он не будет установлен на устройстве.

Для того, чтобы RADIUS-сервер назначил **VLAN**, необходимо сконфигурировать соответствующие параметры на сервере. Для назначения VLAN RFC 3580 определяет следующие атрибуты в пакетах RADIUS.

Параметры для VLAN:

RADIUS Tunnel Attribute	Описание	Значение	Использование
Tunnel-Type	Этот атрибут указывает туннельный протокол, который нужно использовать в качестве инициатора или терминатора туннеля.	13 (VLAN)	Обязательно
Tunnel-Medium-Type	Атрибут указывает используемую транспортную Среду.	6 (802)	Обязательно
Tunnel-Private-Group-ID	Атрибут указывает групповой ID для определенной	string	Обязательно

Если пользователь сконфигурировал атрибут ACL на RADIUS-сервере (например, ACL Script: ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;) и аутентификация 802.1X, WAC или на основе MAC прошла успешно, устройство назначит ACL Script в соответствии с настройками RADIUS-сервера. Вход в режим **Access-List Configuration Mode** и выход из данного режима должны быть парой, в противном случае ACL Script будет отклонен. Дополнительная информация о модуле ACL представлена в **Главе «Команды ACL (Список управления доступом)»**.

Приложение Д. Поддержка атрибутов IETF RADIUS

Для атрибутов RADIUS существуют определенные детали аутентификации, авторизации и конфигурации для запросов и ответов. В данном разделе приведен список атрибутов RADIUS, которые в данный момент поддерживает коммутатор.

Атрибуты RADIUS поддерживаются стандартом IETF и Vendor-Specific Attribute (VSA). VSA позволяет вендорам создавать собственные дополнительные атрибуты RADIUS. Для подробной информации о VSA D-Link обратитесь к **Приложению Г, «Назначение атрибутов RADIUS»**.

Атрибуты RADIUS стандарта IETF определены в RFC 2865 Remote Authentication Dial-In User Service (RADIUS), RFC 2866 RADIUS Accounting, RFC 2868 RADIUS Attributes for Tunnel Protocol Support и RFC 2869 RADIUS Extensions.

Список атрибутов IETF RADIUS, поддерживаемых коммутатором T-KOM, приведен в таблице ниже.

Атрибуты аутентификации RADIUS:

Номер	Атрибут IETF
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
12	Framed-MTU
18	Reply-Message
24	State
26	Vendor-Specific
27	Session-Timeout
29	Termination-Action
30	Called-Station-ID
31	Calling-Station-ID
32	NAS-Identifier
60	CHAP-Challenge
61	NAS-Port-Type
64	Tunnel-Type
65	Tunnel-Medium-Type
77	Connect-Info
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID
85	Acct-Interim-Interval
87	NAS-Port-ID

95	NAS-IPv6-Address
----	------------------

Атрибуты RADIUS Accounting:

Номер	Атрибут IETF
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
31	Calling-Station-ID
40	Acct-Status-Type
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-ID
45	Acct-Authentic
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
52	Acct-Input-Gigawords
53	Acct-Output-Gigawords
61	NAS-Port-Type
95	NAS-IPv6-Address
